TRABAJO DE GRADO

RECOMENDACIONES DE SEGURIDAD PARA LA PREVENCIÓN DE CIBERATAQUES QUE VULNEREN LA INFORMACIÓN DE LOS NIÑOS, NIÑAS, ADOLESCENTES Y JÓVENES DEL INSTITUTO COLOMBIANO PARA LA JUVENTUD

SEBASTIÁN ESPINEL CARRANZA

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

TRABAJO DE GRADO

RECOMENDACIONES DE SEGURIDAD PARA LA PREVENCIÓN DE CIBERATAQUES QUE VULNEREN LA INFORMACIÓN DE LOS NIÑOS, NIÑAS, ADOLESCENTES Y JÓVENES DEL INSTITUTO COLOMBIANO PARA LA JUVENTUD

SEBASTIÁN ESPINEL CARRANZA

Trabajo de grado para optar al título de Especialista en Seguridad de la Información

Docente

ALFONSO LUQUE ROMERO
ESPECIALIZACIÓN
EN SEGURIDAD DE LA INFORMACION

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

1. INTRODUCCIÓN

Las tecnologías de la información sin duda alguna han tenido grandes avances con el pasar de los años, beneficiando de gran manera a la sociedad, sin embargo, dichas tecnologías se encuentran expuestas constantemente a diferentes tipos de amenazas.

En la actualidad muchas empresas no cuentan con una evaluación de riesgos que les ayude a tomar las acciones adecuadas para mitigar cualquier tipo de amenaza que afecte su correcta operación, éste es el caso del Instituto Colombiano para la Juventud (ICPJ). El presente trabajo de investigación nace debido a la necesidad de implementar una adecuada evaluación de riesgos sobre los activos de tecnología críticos de la entidad, con el fin de mejorar la seguridad de la información en dichos activos. abarcando áreas como la ciberseguridad[1] en el ICPJ empresa que ha sido víctima de múltiples ataques informáticos.

Para el desarrollo del presente trabajo se utilizarán las directrices suministradas en la norma técnica colombiana ISO/IEC 27005, la cual es una de las metodologías recomendada por el MinTIC.

[1] Kaspersky, Ciberseguridad, página web, Consultado 01 marzo de 2020 disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

2. GENERALIDADES

1. LÍNEA DE INVESTIGACIÓN

En el programa se trabaja sobre la línea de software inteligente y convergencia tecnológica

2. PLANTEAMIENTO DEL PROBLEMA

Los sistemas informáticos que gestionan los datos sensibles de los usuarios que conforman la entidad, actualmente no cuentan con una adecuada evaluación de riesgos a los cuales se encuentran expuestos constantemente, de tal manera que se evidencie las falencias de ciberseguridad.

Los datos pueden ser utilizados para acciones delictivas, como por ejemplo el robo de la información. Actualmente los procesos de seguridad son ineficaces y desorganizados para proteger los activos informáticos que tienen la información crítica de la entidad, ya que se busca la confidencialidad, disponibilidad e integridad de la información para que su operación sea continua con el fin de atender las necesidades de la comunidad de manera oportuna y efectiva.

2.2.1. ANTECEDENTES DEL PROBLEMA

El malware también conocido como software malicioso hace referencia a toda aplicación o código malicioso el cual es nocivo para los sistemas informáticos, perjudica computadores, servidores, redes y dispositivos móviles, el malware tiene la capacidad de eliminar los datos de los usuarios, cifrarlos, alterar o tener el control de funciones primordiales de los computadores, así como también de observar toda actividad que se realice en éstos sin el consentimiento o conocimiento alguno de los usuarios[2]. El malware es muy utilizado para realizar ciberataques, a continuación, se encuentran los 5 ciberataques más célebres de los últimos 10 años a nivel mundial[3]:

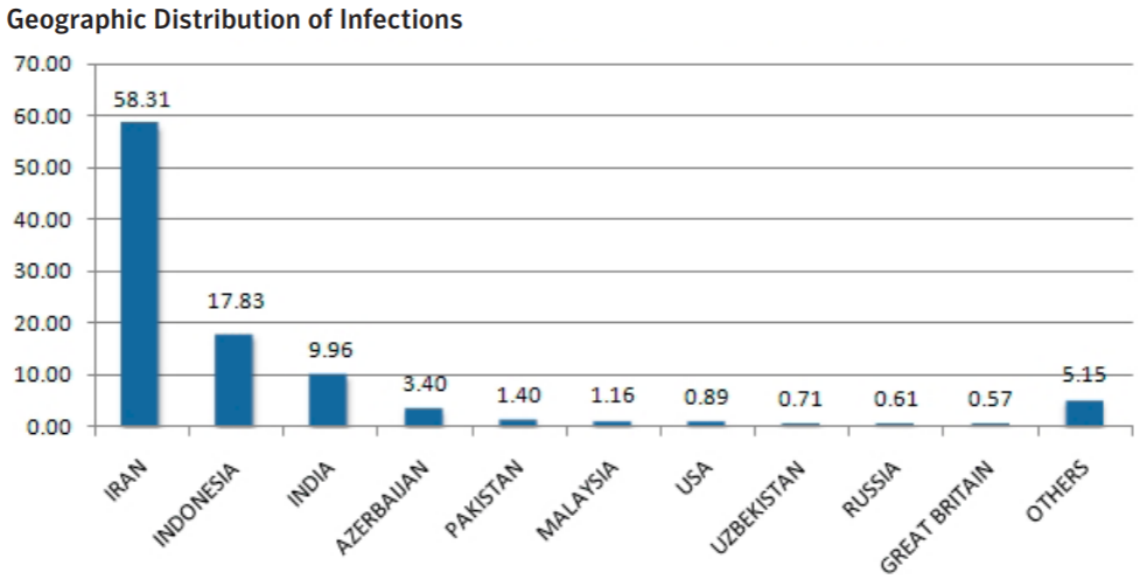
En junio del 2010 se conoció el ciberataque Stuxnet, un malware de tipo gusano, el cual es considerado como el ciberataque más complejo de la historia, fue destinado para operar en contra del programa nuclear de Irán, consiguió desacelerar el proceso de enriquecimiento de uranio en una instalación nuclear iraní conocida como Natanz, inhabilitando las centrifugadoras usadas para

[2] Malwarebytes, Malware, página web, Consultado 01 marzo de 2020 disponible en: https://es.malwarebytes.com/malware/

[3] Kaspersky, five-most-notorious-cyberattacks, página web, Snow John, 07 noviembre 2018, Consultado 12 marzo de 2020 disponible en: https://www.kaspersky.es/blog/five-most-notorious-cyberattacks/17277/

enriquecerse de uranio[4], Stuxnet tenía la capacidad de propagarse de forma oculta haciendo uso de las memorias USB e incluso accediendo a los computadores que no estuvieran conectados a una red local o a internet. Este gusano se propago velozmente a muchos países, infectando cientos de miles de computadores, pero no podía estropearlos puesto que había sido creado para un objetivo muy claro[5]. En la figura 1 se muestran los países que fueron infectados con Stuxnet para el año 2010.

Figura 1. Distribución geográfica de infecciones con Stuxnet en 2010



Fuente: GERSHWIN, Aaron, 31 de julio de 2019. "Stuxnet, or how to destroy a centrifuge with a small piece of code". Disponible desde Internet en: https://hackernoon.com/stuxnet-or-how-to-destroy-a-centrifuge-with-a-small-piece-of-code-66se283f

En el año 2012 el FBI menciono por primera vez ciberataques que tenían como objetivo los huéspedes de hoteles, este tipo de ataque fue denominado como DarkHotel también conocido como Tapaoux, un malware de tipo spyware cuya forma de infiltrarse en los equipos de las victimas era haciendo uso de la red Wi-Fi operando en una gran cantidad de hoteles de lujo[6]. Los huéspedes al conectarse a la red Wi-Fi del hotel, se les realizaba la recomendación de instalar actualizaciones supuestamente legitimas de un software conocido, en el momento que los huéspedes aceptaban dichas actualizaciones sus dispositivos quedaban inmediatamente infectados con DarkHotel, este spyware registraba todas las

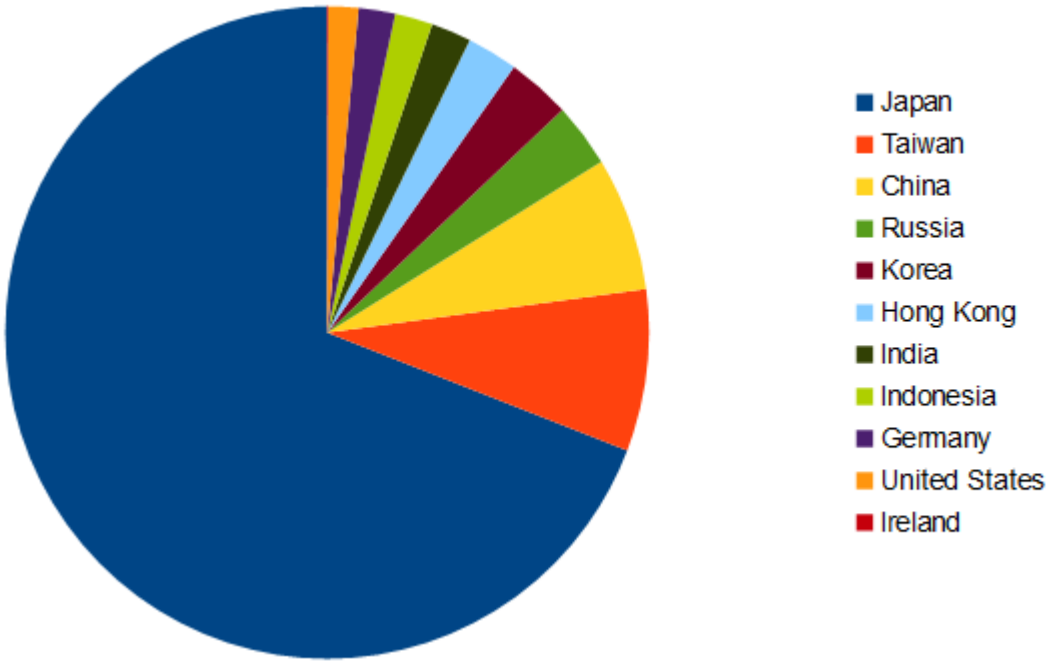
[4] Welivesecurity, sistemas-industriales-en-la-mira, página web, Lipovsky Robert, 20 junio 2017, Consultado 12 marzo de 2020 disponible en: https://www.welivesecurity.com/la-es/2017/06/20/sistemas-industriales-en-la-mira/

[5] Kaspersky, five-most-notorious-cyberattacks, página web, Snow John, 07 noviembre 2018, Consultado 12 marzo de 2020 disponible en: https://www.kaspersky.es/blog/five-most-notorious-cyberattacks/17277/

[6] Kaspersky, darkhotel-espionaje-en-hoteles-de-lujo-asiaticos, página web, Drozhzhin Alex, 10 noviembre 2014, Consultado 12 marzo de 2020 disponible en: https://www.kaspersky.es/blog/darkhotel-espionaje-en-hoteles-de-lujo-asiaticos/4809/

pulsaciones en el teclado permitiendo así que los ciberdelincuentes obtuvieran acceso a información confidencial[7].
Como se puede visualizar en la figura 2, en total fueron once los países fueron afectados por DarkHote en el 2014, siendo Japón el más impactado.

Figura 2. Países más afectados por Darkhotel en 2014

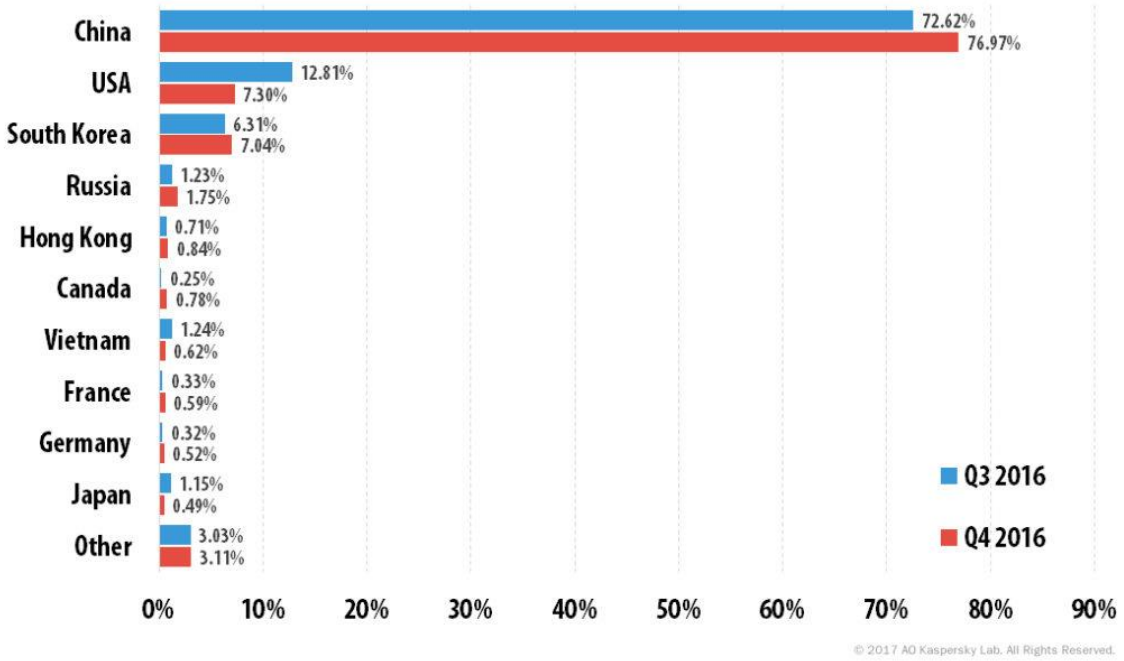


Fuente: DROZHZHIN, Alex, 10 de noviembre de 2014. "DarkHotel: una campaña de espionaje en hoteles de lujo asiáticos". Disponible desde Internet en: https://www.kaspersky.es/blog/darkhotel-espionaje-en-hoteles-de-lujo-asiaticos/4809/

En octubre del año 2016 se presentó el ciberataque Mirai, este malware de tipo botnet afecto principalmente los routers, cámaras IP de vigilancia y grabadoras digitales de video. Mirai fue usado principalmente con el fin de ejecutar ataques de denegación de servicio (DoS) al proveedor de servicios DNS conocido como Dyn. Dyn no tolero dicho ataque por lo cual muchos servicios que dependían de él se inhabilitaron como, por ejemplo: Netflix, Spotify, Twitter, PayPal, entre muchos más[8]. En total 80 países fueron víctimas de este ciberataque sin embargo los países más atacados por Mirai fueron 10 como se puede observar en la figura 3, dichos países representaron 96.9% de todos los ataques[9].

[7] Kaspersky, five-most-notorious-cyberattacks, página web, Snow John, 07 noviembre 2018, Consultado 12 marzo de 2020 disponible en: https://www.kaspersky.es/blog/five-most-notorious-cyberattacks/17277/
[8] Ibíd., p.1
[9] Securelist, ddos-attacks-in-q4-2016, página web, Khalimonenko Alexander, Strohschneider Jens, Kupreev Oleg, 02 febrero 2017, Consultado 12 marzo de 2020 disponible en: https://securelist.com/ddos-attacks-in-q4-2016/77412/

Figura 3. Distribución de ataques por país, tercer semestre de 2016 frente a cuarto trimestre de 2016
Q3: Tercer Trimestre - Q4: Cuarto Trimestre

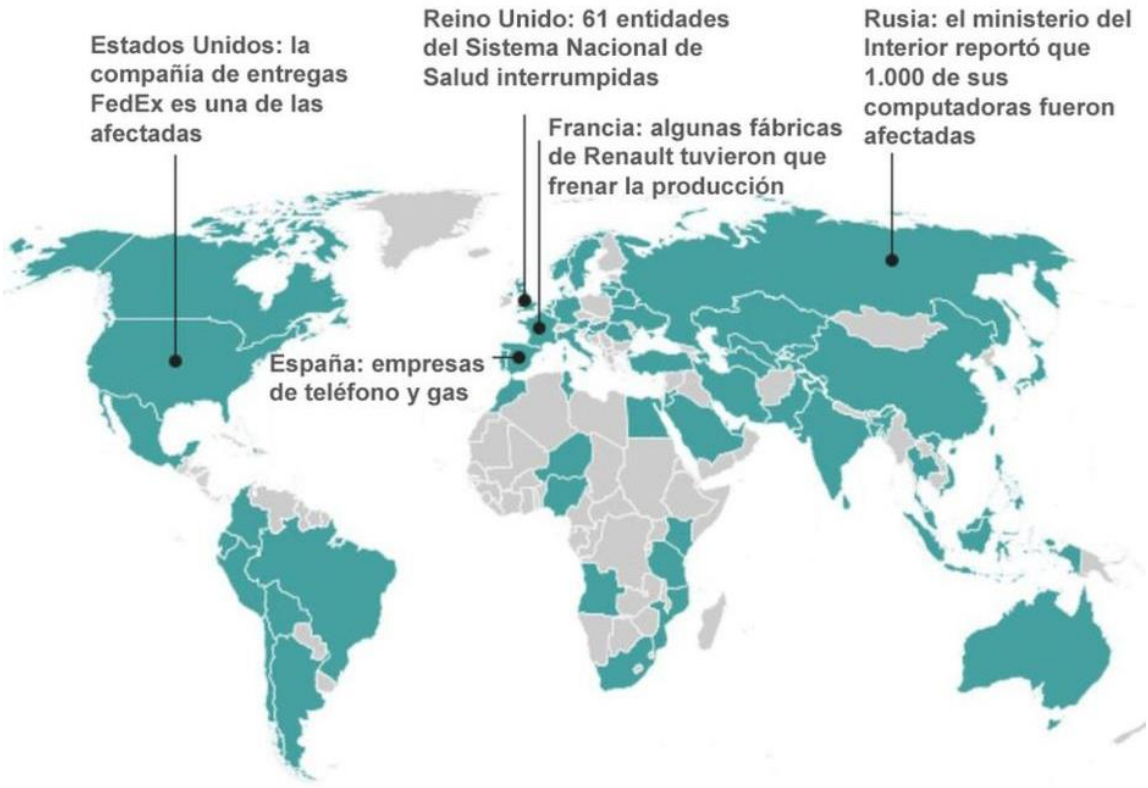


Fuente: Khalimonenko, Alexander, Strohschneider, Jens, Kupreev, Oleg, 02 de febrero de 2016. "DDoS attacks in Q4 2016". Disponible desde Internet en: https://securelist.com/ddos-attacks-in-q4-2016/77412/

En el mes de mayo del año 2017 un ciberataque dio a conocer a WannaCry, un tipo de malware de tipo ransomware que se transfiere por las redes hasta llegar a los computadores, llegado a ese momento es capaz de encriptar la información o lo que es peor los usuarios no podían iniciar la sesión en sus computadores. WannaCry afecto a más de 150 países siendo Rusia, India, China y Brasil los países más perjudicados, algunas de las compañías perjudicadas fueron Renault, Telefónica, Hitachi, FedEX, el NHS (entidad responsable de prestar el servicio de salud) del reino unido y Deutsche Bahn[10].Los países que se vieron afectados por Wannacry en las primeras horas se muestran en la figura 4.

[10] Avast, c-wannacry, página web, Consultado 12 marzo de 2020 disponible en: https://www.avast.com/es-es/c-wannacry

Figura 4. Países afectados en las primeras horas del ciberataque WannaCry en 2017



Fuente: BBC Mundo, 15 de mayo de 2017. "Ciberataque masivo: ¿quiénes fueron los países e instituciones más afectados por el virus WannaCry?". Disponible desde Internet en: https://www.bbc.com/mundo/noticias-39929920

En tan solo 4 días este malware logró dejar fuera de servicio más de 200.000 mil computadores en 150 países, incluyendo infraestructuras criticas como en hospitales donde encripto todos los dispositivos incluso el equipo médico[11].

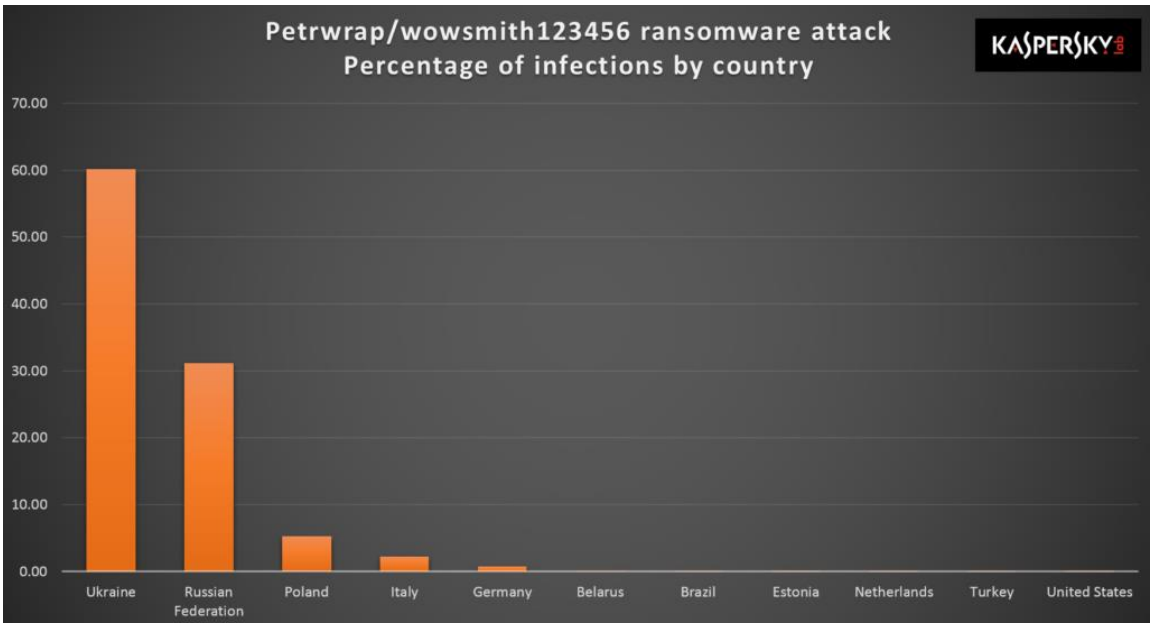
A principios del verano del 2017 se presentó el ciberataque NotPetya, un malware similar a Wannacry con la diferencia de que NotPetya puede bloquear el disco duro de un equipo por completo, evitando así que el ordenador se inicie. NotPetya es una variante del malware Petya el cual apareció por primera vez a inicios del año 2016. NotPetya es un tipo de malware que se conoce como Wiper, comenzó a propagarse en organizaciones de Ucrania para posteriormente extenderse por Europa y Estados Unidos[12]. Los ciberdelincuentes obtuvieron el control sobre un servidor de actualizaciones de un software financiero conocido como MeDoc, consiguiendo de esta manera que muchos clientes que usaban dicho software

[11] Kaspersky, five-most-notorious-cyberattacks, página web, Snow John, 07 noviembre 2018, Consultado 12 marzo de 2020 disponible en: https://www.kaspersky.es/blog/five-most-notorious-cyberattacks/17277/

[12] Avast, c-petya, página web, Consultado 12 marzo de 2020 disponible en: https://www.avast.com/c-petya

recibieran el malware NotPetya oculto en las actualizaciones del software MeDoc, para posteriormente propagarse rápidamente por la red. Se estima que el daño del ciberataque NotPetya tuvo un valor por 10.000 millones de dólares, mientras que el de WannaCry se encuentra entre 4.000 y 8.000 millones de dólares, siendo esto así se puede afirmar que NotPetya es el ciberataque más costoso hasta el momento[13]. En la figura 5 se ilustra el porcentaje de infecciones por país para el año 2017.

Figura 5. Porcentaje de infecciones por país / Notpetya en 2017



Fuente: GREAT, 27 de junio de 2017. "Schroedinger's Pet(ya)". Disponible desde Internet en: https://securelist.com/schroedingers-petya/78870/

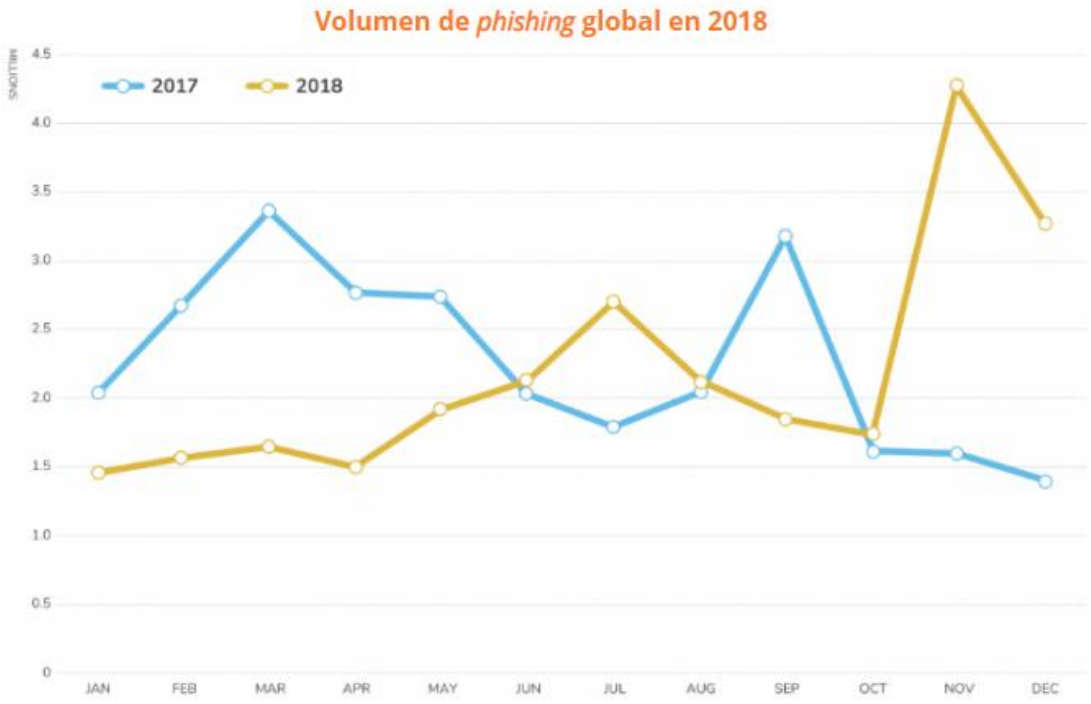
Existen varios métodos que los ciberdelincuentes utilizan para realizar una cantidad considerable de ciberataques, este es el caso del phishing, un método que es usado para engañar a las personas y de esta manera conseguir información confidencial, como datos de tarjetas de crédito, números de cuentas bancarias, claves, etcétera. Lo logran a través del envío de correos electrónicos engañosos o dirigiendo a las personas hacia un sitio web falso. Los mensajes de phishing tratan de imitar organizaciones legales como agencias del gobierno, bancos, etcétera, solicitando cordialmente que las personas actualicen, verifiquen o confirmen sus datos, posteriormente se le redirige a una página web fraudulenta y una vez que las personas ingresen su información, esta es robada[14].

[13] Kaspersky, five-most-notorious-cyberattacks, página web, Snow John, 07 noviembre 2018, Consultado 12 marzo de 2020 disponible en: https://www.kaspersky.es/blog/five-most-notorious-cyberattacks/17277/

[14] Avast, c-phishing, página web, Consultado 12 marzo de 2020 disponible en: https://www.avast.com/es-es/c-phishing

De acuerdo al informe de ciberamenazas SonicWall 2019, en el 2018 se registraron 26 millones de ataques de phishing en todo el mundo, lo cual significa que existe una caída del 4.1% respecto al 2017[15], esto se puede visualizar en la figura 6.

Figura 6. Volumen de phishing global en 2018



Fuente: SonicWall, 28 de mayo de 2019. "Dentro de las campañas de phishing modernas de 2019". Disponible desde Internet en: https://blog.sonicwall.com/es-mx/2019/05/inside-the-modern-phishing-campaigns-of-2019/

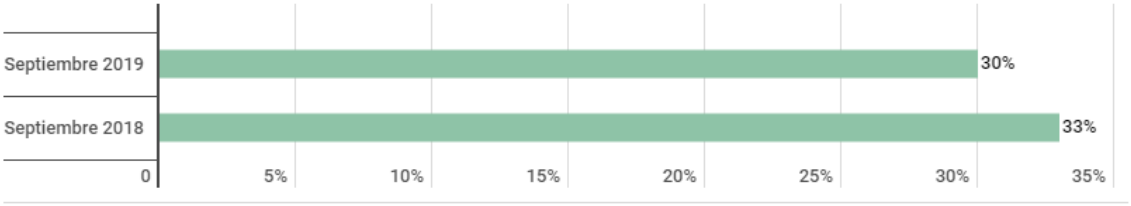
Otro de los métodos de ciberataques más utilizados, son los ataques de denegación de servicio (DoS) en el segundo trimestre del año 2019 se presentó el ataque de este tipo más extenso hasta el momento, teniendo una duración de 509 horas, lo que equivale a más de 21 días, de acuerdo al informe trimestral sobre ataques de este tipo elaborado por la compañía Kaspersky, entre los meses de Abril y Junio de 2019 el número total de ataques de denegación de servicio aumento en un 18% comparado al mismo periodo del año 2018[16]. En la figura 7 se visualiza la cantidad y distribución de los ataques de denegación de servicio en septiembre de 2019 comparado con septiembre de 2018.

[15] Sonic Wall, inside-the-modern-phishing-campaigns-of-2019, página web, Consultado 12 marzo de 2020 disponible en: https://blog.sonicwall.com/es-mx/2019/05/inside-the-modern-phishing-campaigns-of-2019/

[16] Europa Press, noticia-ataque-ddos-mas-largo-historia-sido-2019-duro-509-horas, 07 agosto 2019, página web, Consultado 12 marzo de 2020 disponible en: https://www.europapress.es/portaltic/ciberseguridad/noticia-ataque-ddos-mas-largo-historia-sido-2019-duro-509-horas-20190807160911.html

El ataque más largo del último trimestre de 2019 tuvo como objetivo un proveedor de comunicaciones chino, este ataque tuvo una duración de 11.6 días lo que equivale a 279 horas, un tiempo 1.8 veces inferior comparado al segundo trimestre de ese mismo año[17].

Figura 7. Cantidad y distribución estadística de los ataques DoS en septiembre de 2019 y 2018



Fuente: IBRAGIMOV, Timur, KUPREEV, Oleg, BADOVSKAYA, Ekaterina, GUTNIKOV, Alexander, 11 de noviembre de 2019. "Los ataques DDoS en el tercer trimestre de 2019". Disponible desde Internet en: https://securelist.lat/ddos-report-q3-2019/89671/

Otro de los métodos utilizados por los ciberdelincuentes consiste en el ataque denominado Man in the Middle o ataque intermediario, consiste en que el ciberdelincuente interviene el tráfico de datos de dos usuarios en una comunicación suplantando la identidad de uno u otro, de esta manera les hace creer que se están comunicando entre ellos. Este tipo de ataques se efectúan en redes informáticas con el objetivo de invalidar la codificación y poder ingresar a la información confidencial, como contraseñas, números de cuentas bancarias, etcétera. En la figura 8 se puede visualizar el croquis básico correspondiente a un ataque Man in the Middle[18].

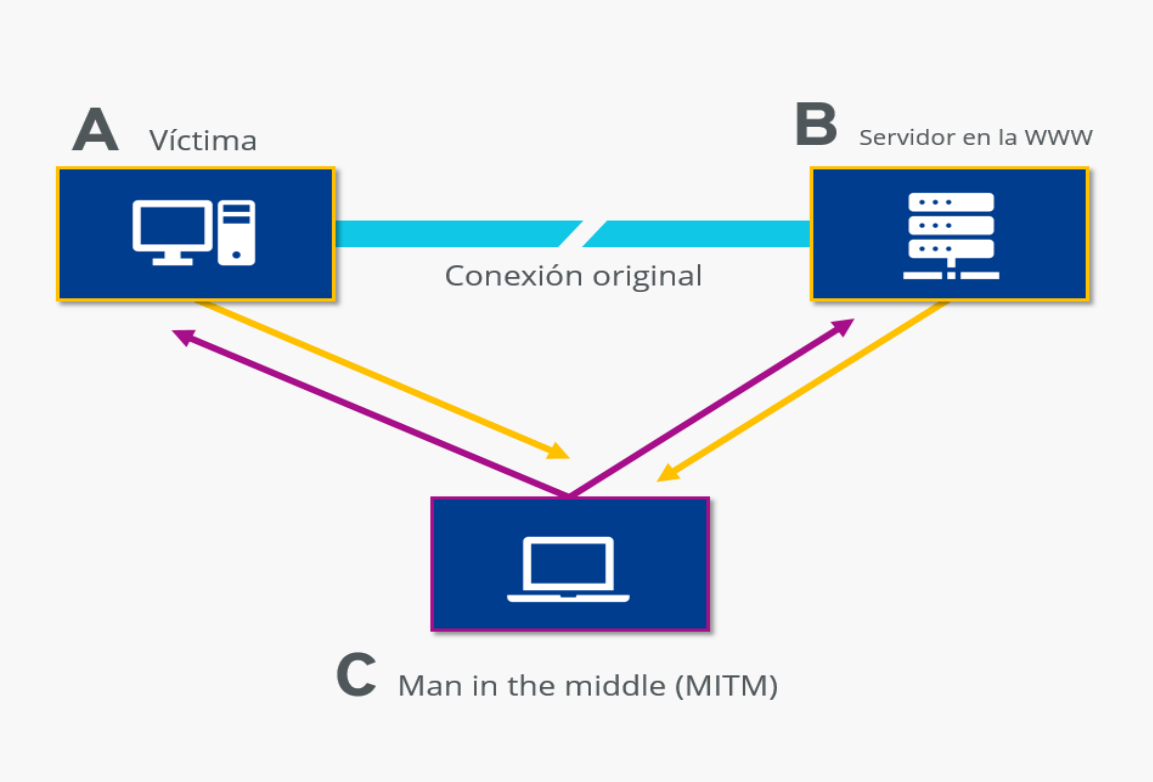
Man in the Middle es muy usado en ataques en redes wifi públicas las cuales son muy vulnerables, muchas personas se conectan a ellas y los ciberdelincuentes pueden obtener información personal de los usuarios[19].

[17] Securelist, ddos-report-q3-2019, página web, Ibragimov Timur, Kupreev Oleg, Badovskaya Ekaterina, Gutnikov Alexander, 11 noviembre 2019, Consultado 12 marzo de 2020 disponible en:
https://securelist.lat/ddos-report-q3-2019/89671/

[18] Ionos, ataques-man-in-the-middle-un-vistazo-general, página web, 19 marzo 2019, Consultado 12 marzo de 2020 disponible en:
https://www.ionos.es/digitalguide/servidores/seguridad/ataques-man-in-the-middle-un-vistazo-general/

[19] Un fantasma en el sistema, mitm-ataque-man-in-the-middle, página web, 06 diciembre 2019, Consultado 12 marzo de 2020 disponible en:
https://www.unfantasmaenelsistema.com/2019/12/mitm-ataque-man-in-the-middle/

Figura 8. Ataque Man in the Middle



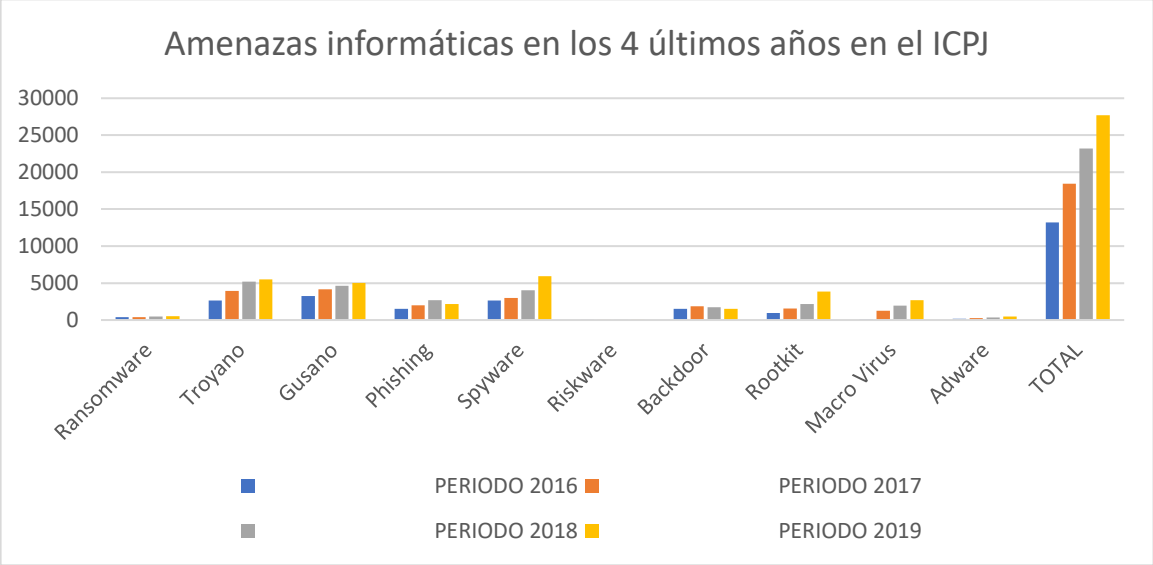
Fuente: IONOS, 19 de marzo de 2019. "Ataque man-in-the-middle: modalidades y medidas de defensa". Disponible desde Internet en: https://www.ionos.es/digitalguide/servidores/seguridad/ataques-man-in-the-middle-un-vistazo-general/

En los últimos 4 años se han presentado diferentes tipos de ciberataques en el ICPJ para un total de 13211, 18451, 23186 y 27699 ciberataques detectados en los años 2016, 2017, 2018 y 2019 respectivamente, como se ilustra en el gráfico de la figura 9 cada año van en aumento los ciberataques que afectan considerablemente el ICPJ, siendo el malware de tipo ransomware el que más impacto ha tenido en la entidad, ocasionando graves daños como la pérdida total de la información, lo cual origino la detención de muchos procesos importantes de la entidad ICPJ, seguido del ransomware el phishing es el otro tipo de malware que más impacto en la entidad, los ciberdelincuentes suplantan la entidad de una persona o una empresa para engañar a los funcionarios con el fin de robarles su información personal, de acuerdo al centro cibernético de la policía nacional en Colombia los incidentes más reportados a nivel nacional son los casos de Phishing con un 42%[20]. Otros tipos de malware como troyanos, gusanos, spyware, adware, etcétera, igualmente han afectado el desarrollo de las actividades de los

[20] Policía Nacional de Colombia, Tendencias cibercrimen 2019 - 2020, página web, Consultado 12 marzo de 2020 disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

funcionarios del ICPJ, a pesar de contar con un antivirus en la entidad muchos computadores asignados a los funcionarios tienen un sistema operativo totalmente obsoleto como por ejemplo: Windows XP, cuyo soporte finalizo desde el 8 de abril de 2014[21], Windows Server 2003 que ya no cuenta con soporte desde el 14 de Julio de 2015[22], Windows Server 2008 cuyo soporte termino el 14 de enero de 2020[23] y Windows 7 que de igual manera no cuentan con soporte desde el 14 de enero de 2020 por parte de su fabricante Microsoft[24], convirtiendo estos sistemas operativos en un objetivo fácil de vulnerar por parte de los ciberdelincuentes.

Figura 9. Amenazas informáticas en los 4 últimos años en el ICPJ



Fuente: Área de Tecnología ICPJ, 01 de febrero de 2020, "Informe de amenazas detectadas en la entidad en los últimos 4 años"

[21] Microsoft, end-of-windows-xp-support, página web, Consultado 12 marzo de 2020 disponible en: https://www.microsoft.com/es-co/microsoft-365/windows/end-of-windows-xp-support

[22] Ciset, 311-fin-del-soporte-a-windows-server-2003, página web, 14 mayo 2019, Consultado 12 marzo de 2020 disponible en: https://www.ciset.es/publicaciones/blog/311-fin-del-soporte-a-windows-server-2003

[23] Microsoft, windows-server-2008, página web, Consultado 12 marzo de 2020 disponible en: https://www.microsoft.com/es-es/cloud-platform/windows-server-2008

[24] Microsoft, windows-7-support-ended-on-january-14-2020, página web, 15 enero 2020, Consultado 12 marzo de 2020 disponible en: https://support.microsoft.com/es-co/help/4057281/windows-7-support-ended-on-january-14-2020

2.2.2. PREGUNTA DE INVESTIGACIÓN

¿Cómo proteger la información de los niños, niñas, jóvenes y adolescentes de la entidad frente a las diferentes amenazas informáticas a las que está expuesta?

2.2.3. VARIABLES DEL PROBLEMA

Activos informáticos: Son los recursos de hardware y software que pertenecen a una empresa y que a través de ellos la entidad puede realizar muchos de sus procesos, dichos recursos son susceptibles a diferentes tipos de ciberataques.

Ciberseguridad: Es la manera de proteger los equipos informáticos, dispositivos inteligentes, las redes y la información digital de ciberataques[25].

Ciberataques: son acciones ofensivas contra los sistemas informáticos en el ciberespacio y que buscan infectar equipos para acceder y tener el control de una o varias máquinas. Con el fin de encriptar y secuestrar información a cambio de recompensas económicas.[26]

Amenazas informáticas: Una amenaza informática es cualquier actividad que pueda conducir a la pérdida, corrupción o robo de los datos hasta la interrupción de los sistemas informáticos.

Controles de seguridad: Son medidas que se toman para reducir los riesgos de seguridad de la información, como violaciones de los sistemas de información, robo de datos y cambios no autorizados en la información o los sistemas digitales. Estos controles de seguridad están destinados a ayudar a proteger la disponibilidad, la confidencialidad y la integridad de los datos y las redes.

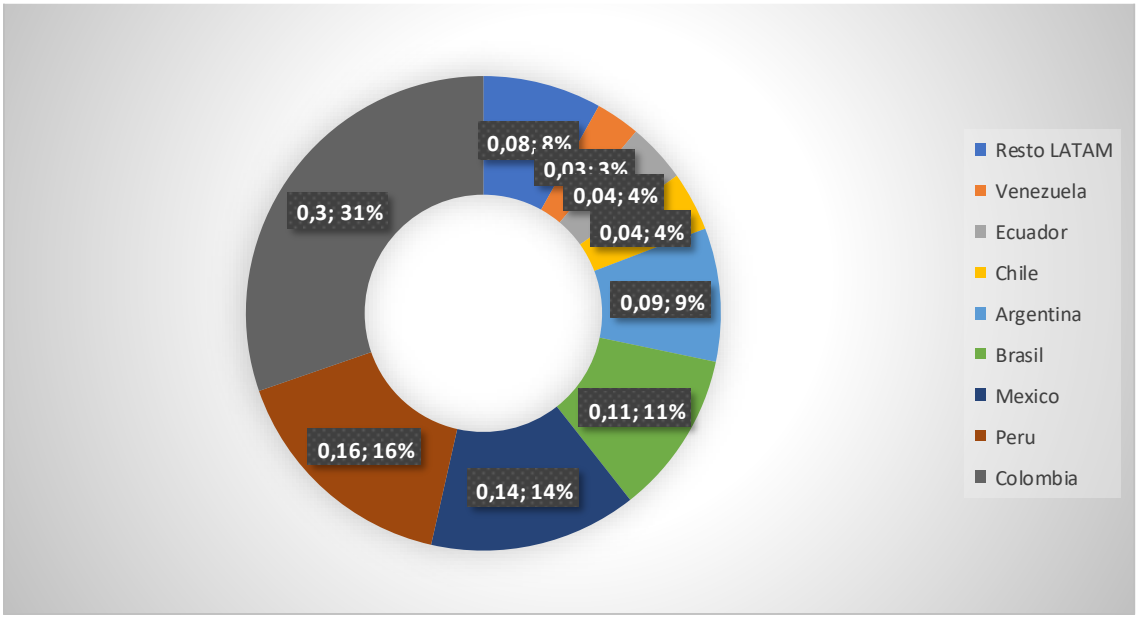
[25] Mendoza, Miguel, ciberseguridad, página web, Consultado el 30 de mayo de 2020 disponible en: https://www.economiasimple.net/glosario/ciberseguridad

[26] Caser, que-es-un-ciberataque-y-tipos, página web, Consultado 12 marzo de 2020 disponible en: https://www.caser.es/seguros-empresas/articulos/que-es-un-ciberataque-y-tipos

3. JUSTIFICACIÓN

Según la policía nacional y su centro cibernético, en el año 2019 Colombia fue víctima del 30% de ataques de tipo ransomware en Latinoamérica, seguido de Perú con el 16%, México 14%, Brasil 11% y Argentina 9%, también se identificó que las empresas medianas son las preferidas por los cibercriminales puesto que los niveles de seguridad de éstas por lo general suelen ser bajos como se observa en la figura 10[27].

Figura 10. Países más afectados por ransomware en Latinoamérica



Fuente: GIUSTO BILIĆ, Denise, 04 de junio de 2019. "Países más afectados por el ransomware en Latinoamérica durante 2018". Disponible desde Internet en: https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/

Se presenta el siguiente trabajo de grado por la necesidad que tiene la entidad ICPJ para mejorar la ciberseguridad de su infraestructura ya que la empresa ha sido víctima de múltiples ciberataques que impactan seriamente en su operación para atender las necesidades de su comunidad y cuidar el prestigio de su misión encaminada a la protección los derechos de los niños y adolescentes.

En el área de tecnología del ICPJ se ha identificado que a través de las memorias USB, el correo electrónico, el ingreso a páginas web de reputación incierta y descargas de aplicaciones de las mismas son los medios más usados por los ciberdelincuentes para poder contagiar los equipos informáticos con malware y así poder realizar los ciberataques, a continuación, se presenta en la tabla 1 y en

[27] Ceballos, Adriana. Tendencias cibercrimen en Colombia. En línea. 29 octubre de 2019. 23 abril 2020. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

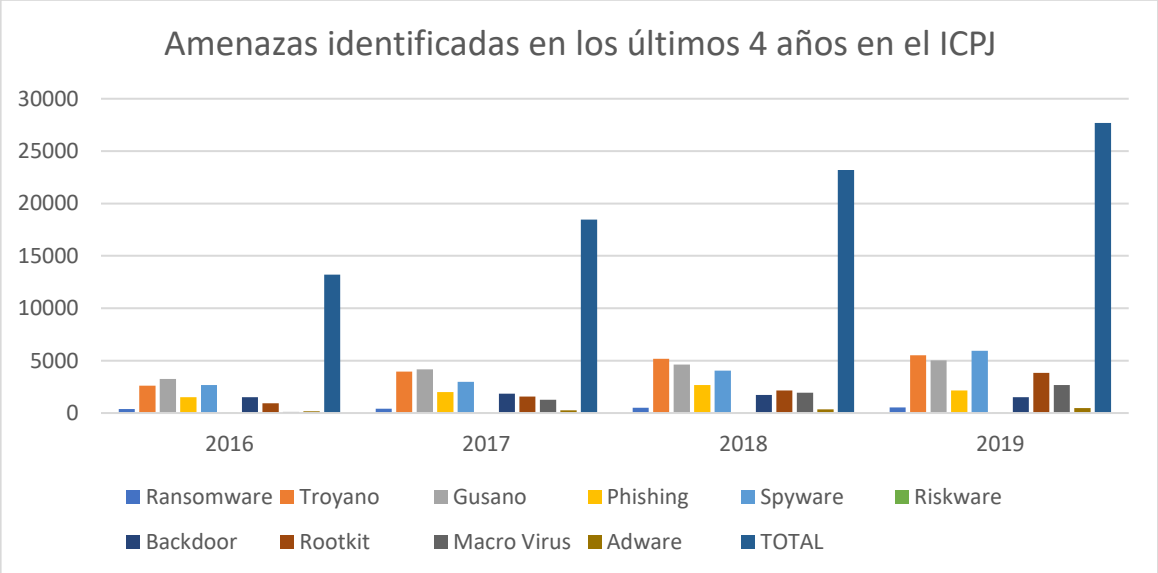
la figura 11, los tipos de amenazas, periodo, números de ciberataques y el total de estos identificados en los 4 últimos años en la entidad:

Tabla 1. Total de amenazas identificadas en el ICPJ en los últimos años

	PERIODO			
TIPO DE AMENAZA	**2016**	**2017**	**2018**	**2019**
RANSOMWARE	391	406	489	534
TROYANO	2623	3945	5178	5517
GUSANO	3256	4159	4628	5021
PHISHING	1520	1987	2676	2157
SPYWARE	2661	2982	4037	5934
RISKWARE	3	14	12	10
BACKDOOR	1523	1846	1724	1519
ROOTKIT	945	1574	2149	3846
MACRO VIRUS	121	1274	1952	2675
ADWARE	168	264	341	486
TOTAL	13211	18451	23186	27699

Fuente: Área de Tecnología ICPJ, 30 de octubre de 2020, "Informe de amenazas detectadas en la entidad en los últimos 4 años"

Figura 11. Crecimiento de amenazas identificadas en el ICPJ



Fuente: Área de Tecnología ICPJ, 01 de febrero de 2020, "Informe de amenazas detectadas en la entidad en los últimos 4 años"

Como se puede apreciar el número de ciberataques en el ICPJ cada vez aumentan en la entidad.

3. OBJETIVOS

1. OBJETIVO GENERAL

Definir e implementar estrategias de seguridad informática que permitan prevenir, eliminar y/o bloquear las amenazas para que la información crítica del ICPJ se encuentre disponible, sea integra y confidencial.

2. OBJETIVOS ESPECÍFICOS

1. Realizar la identificación de los activos informáticos que gestionan la información digital de los niños y jóvenes que utilizan los servicios de la entidad para analizar y establecer los riesgos asociados.

2. Efectuar la evaluación de riesgos a los activos informáticos que administran la información misional de la entidad utilizando la norma técnica ISO 27005 sugerida por el MinTIC.
3. Definir e implementar estrategias de seguridad que permitan prevenir la ocurrencia de ciberataques.

4. MARCOS DE REFERENCIA

1. MARCO CONCEPTUAL

El gran avance que han tenido las tecnologías de la información y comunicación (TIC), se ha venido presentando de una manera excepcional, las innovaciones en el campo de las TICS por lo general tienen un impacto positivo en la calidad de vida y del trabajo de las personas, las empresas deben contar con una infraestructura tecnológica para poder realizar una gran parte de sus procesos, sin embargo existen diferentes tipos de vulnerabilidades y amenazas a las cuales se encuentran expuestas las infraestructuras tecnológicas de las empresas, las probabilidades de que las amenazas se manifiesten sobre dichas infraestructuras causando perjuicios o daños[28] estarán siempre presentes.

En el presente trabajo de investigación, se utilizará una evaluación de riesgos como instrumento para mejorar las condiciones de seguridad de la infraestructura tecnológica que gestiona la información Core del ICPJ, por lo tanto, es relevante identificar, analizar y entender los diferentes tipos de amenazas y vulnerabilidades que afectan dicha estructura.

Como primera instancia encontramos el malware, se trata de cualquier software que pueda representar una amenaza al sistema o daño informático para el usuario final, por lo general el malware se propaga a través de dos tipos de vulnerabilidades, las cuales se relacionan a continuación:

En primera instancia encontramos las vulnerabilidades de software, se enfoca en explotar debilidades del sistema operativo o de algún programa, ciertos tipos de malware tienen la capacidad de replicarse a sí mismos con el fin de dirigirse automáticamente a través de la red para infectar a la mayor cantidad de equipos conectados, el malware puede cambiar la manera de funcionar de un ordenador o también de modificar, alterar o eliminar la información que este almacena y/o procesa[29]. En segunda instancia encontramos las vulnerabilidades asociadas a las personas, en su gran mayoría son los propios usuarios quienes, con su desconocimiento o exceso de confianza, contribuyen a la propagación de software malicioso, puede haber un equipo operativo con la mayor seguridad del mundo y que cuente con un antivirus actualizado, pero si las personas que lo utilizan son descuidadas hay índices altos de infectarse y generar perdidas tanto financieras como productivas en las organizaciones.

---

[28] Davara, Fernando, riesgos-vs-amenazas-de-que-se-trata-realmente, página web, Consultado 29 mayo de 2020 disponible en: https://fernandodavara.com/riesgos-vs-amenazas-de-que-se-trata-realmente/

[29] Gema, Gasco. Seguridad informática: Software malicioso. Segunda edición. Madrid: MACMILLAN, 2013. 113p.

El malware puede clasificarse según el impacto sobre la víctima, atendiendo a este criterio, se distingue tres niveles de peligrosidad: bajo, medio o elevado[30].

Para evaluar su nivel de impacto de un espécimen, se estudia la gravedad de las acciones que ocasiona sobre un equipo infectado, su velocidad y facilidad de propagación, así como la cantidad de infecciones producidas recientemente[31].

Según su propagación,

En 1984 el Dr. Fred Cohem clasifico a los emergentes virus de computadoras en tres categorías:

1. Caballos de troya
2. Gusanos
3. Virus

A continuación, se encuentran los diferentes tipos de malware más comunes con su respectiva descripción:

Troyano: Es una aplicación informática supuestamente inofensiva la cual se usa con el fin de obtener datos confidenciales o para piratear el sistema operativo[32].

Gusano: Es un tipo de software malicioso el cual tiene la capacidad de propagarse de manera automática[33].

Para poder propagarse el gusano usa los agujeros de seguridad existentes en redes informáticas y sistemas operativos[34], actualmente este tipo de malware infecta los dispositivos a través del correo electrónico o enlaces sospechosos.

Principales formas de difusión son:

1. Programa de mensajería.
2. Redes P2P.
3. Correo electrónico.
4. Recursos compartidos a través de una red local.

[30] Ibíd., p.114
[31] Ibíd., p.114
[32] Ibíd., p.116
[33] Ibíd., p.115
[34] Ibíd., p.115

Virus informático: Es un software cuya finalidad es la de alterar el correcto funcionamiento de un equipo, sin que el usuario se percate, infectando otros archivos de los sistemas para cambiarlos o modificar archivos personales alojados en los equipos[35].

Spyware: proviene de dos palabras espía y software, se encuentra diseñado para obtener datos personales tales como contraseñas, información de inicios de sesión, tarjetas crédito, débito, entre otros[36].

Adware: proviene de ad y software, se encarga de mostrar publicidad engañosa a las personas de manera abrupta, como, por ejemplo, en forma de ventanas emergente, se suele utilizar para esconder la acción de otro malware[37].

Ransomware**:** se encarga de bloquear y cifrar la información de un equipo o dispositivo con el fin de exigir un pago para poder restaurarla, en la mayoría de los casos los ciberdelincuentes establecen un tiempo determinado para que usuarios paguen y así puedan recuperar sus datos, existe el riesgo de que si se paga lo exigido los ciberdelincuentes no restauren la información[38].

De igual manera es indispensable conocer los términos que pueden ayudar al correcto desarrollo del presente proyecto, a continuación, se relacionan la descripción de dichos términos:

Activo: Es cualquier elemento valioso que tenga una organización, puede tratarse de una base de datos, contraseñas, claves de cifrado, documentos digitales o en papel, computadores, servidores, cintas de backups, entre otros[39].

Riesgo: Es la probabilidad de que se origine un incidente de seguridad, materializándose en una amenaza y causando perdidas o daños al sistema informático.

Para evaluar estos riesgos se hace uso de 2 tipos de análisis, cualitativo cuantitativo, realizando contramedidas como la mitigación, aceptación, transferencia, evitación con el propósito de tratarlos de manera adecuada en la reducción y prevención de las amenazas de ciberseguridad[40].

---

[35] CCFGlobal, que-es-un-virus-informático, página web, Consultado 12 marzo de 2020 disponible en: https://edu.gcfglobal.org/es/virus-informaticos-y-antivirus/que-es-un-virus-informatico/1/

[36] Gema, Gasco. Seguridad informática: Software malicioso. Segunda edición. Madrid: MACMILLAN, 2013. 117p.

[37] Ibíd., p.117

[38] Norton, What is ransomware and how to help prevent ransomware attacks, página web, Consultado 12 marzo de 2020 disponible en: https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html

[39] Ibíd., p.15

[40] Gema, Gasco. Seguridad informática: Software malicioso. Segunda edición. Madrid: MACMILLAN, 2013. 12p.

Delito Informático (Cibercrimen): Es toda actividad ilícita, realizada a través de equipos y aplicaciones informáticas con el objetivo de realizar una estafa o robo usando el internet41.

Ciber-protección: Es la manera de estar protegido frente a diferentes tipos de amenazas digitales[42].

Ciber-seguridad: De acuerdo a ISACA, es una capa de protección para la información, se pretende evitar todo tipo de amenazas que pongan en riesgo la información digital que se encuentre en cualquier dispositivo[43].

Ciber-espacio: Es un entorno virtual el cual se da a través de la interacción de las personas, aplicativos o software y servicios de Internet haciendo uso de equipos, dispositivos móviles y redes conectadas al mismo tiempo[44].

Phishing**:** Proceso fraudulento en el que se intenta extraer información exclusiva, privada o personal suplantando una persona o entidad digitalmente, utilizan el correo electrónico para él envió de múltiples correos como canal para suplantar al remitente de la manera más real posible con descargas de aplicaciones maliciosas o mediante el engaño a sus víctimas con links hacia páginas fraudulentas con el objetivo de efectuar el robo de credenciales e información personal[45].

Vulnerabilidad**:** Es una debilidad de un sistema o activo la cual puede ser aprovechada por atacantes o delincuentes[46].

---

[41] Ibíd., p.17

[42] Ibíd., p.17

[43] Lanz, Leona, 22 de mayo de 2018, que-es-la-ciberseguridad, página web, Consultado 12 marzo de 2020 disponible en: https://openwebinars.net/blog/que-es-la-ciberseguridad/

[44] Gema, Gasco. Seguridad informática: Software malicioso. Segunda edición. Madrid: MACMILLAN, 2013. 18p.

[45] Ibíd., p.20

[46] Ibíd., p.23

Vulnerabilidades de aplicaciones: surgen por bugs en el sistema operativo o codificación de la aplicación; las empresas buscan corregir estos fallos mediante parches o actualizaciones de seguridad, es frecuente que se originen nuevas vulnerabilidades, estas estimulan al desarrollo de actualizaciones para remediar estos errores de programación que pueden aprovechar los hackers[47].

En el año 2015, un fallo denominado SYNful Knock, se encontró en Cisco IOS. Lo que permitió controlar los routers a nivel empresarial. Los hackers lograron monitorear las comunicaciones de red e infectaron otros dispositivos de la red. Esta vulnerabilidad se produjo en el sistema cuando una versión modificada de IOS se incorporó en los routers[48].

Las empresas tienen sistemas informáticos de prueba para la penetración y que solo se utilizan para encontrar y corregir los fallos de software antes de que tomen ventaja y logren explotar el fallo [49].

Clasificación de las vulnerabilidades en la seguridad: Desbordamiento de un búfer: este fallo se produce cuando gran cantidad de información supera los límites de un búfer. Los búferes son espacios de memoria entregada a una aplicación. Al actualizar los datos que sobrepase los límites de un búfer, la aplicación accede a la memoria asignada a otros procesos. Esto origina un bloqueo del sistema, afectando los datos y produciendo el escalamiento de los privilegios en el sistema[50].

Entrada no validada: Es una manera utilizada frecuentemente para verificar datos potencialmente peligrosos con el fin de garantizar que las entradas que se procesen sean llevadas de forma segura dentro del código de la aplicación[51].

[47] Walter, Velasco. Políticas y seguridad de información. En línea. 2 septiembre de 2008. 26 abril de 2020. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

[48] Auchard, Eric. Descubren vulnerabilidad de routers cisco ante ataques informáticos. En línea. 15 septiembre de 2015. 27 de abril de 2020. Disponible en: https://lta.reuters.com/articulo/internet-tecnologia-cisco-idLTAKCN0RF19620150915

[49] Monsalve, Julián. Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento, Boyacá. 2014. 72 páginas. Trabajo de grado. Universidad Santo Tomas. Tunja.

[50] Mora, David. Técnicas de ofensa y defensa a los fallos por corrupción de memoria. Medellín. Trabajo de grado. Universidad de Medellín.

[51] Urbina, Gabriel. Introducción a la Seguridad informática. Segunda edición: San Juan,2016. 160 p.

Condiciones de carrera: Ocurre cuando dos, tres o más procesos pueden acceder a datos los cuales se encuentran compartidos e intentar cambiarlos al mismo tiempo.

Debilidades en las prácticas de seguridad: Todo sistema informático debe proteger sus datos con métodos como autenticación, encriptación, autorización. Los programadores de software pueden realizar un control en los formularios para evitar inyecciones SQL mediante expresiones regulares u otros métodos.

Ataques MITM (Man-In-The-Middle, intermediario): En la conexión entre dos equipos informáticos en el que se interpone un tercero que funciona como un puente para acceder a paquetes intercambiados que se transmitan mediante este. El atacante se interpone en el tráfico entre el origen y destino de dos siguientes maneras[52].

1) Hardware el hacker tiene acceso directo a un componente de red que hace parte del camino entre el origen y el destino.

2) Software: el hacker realiza un engaño para que el origen crea que él es el destino y también consigue qué el destino conciba que él es el origen.

ARP spofing: consiste en imponer cambios en el ARP de la víctima, ARP proviene del protocolo de resoluciones que utiliza para proporcionar una dirección MAC dada para la redirección IP, cada host cliente o servidor tiene una dirección y una tabla ARP[53].

También conocida como cache que almacena pares de IP y MACS, cuando una computadora tiene que resolver una MAC desde una direcciona IP se realiza una solicitud al ARP a la dirección del broadcast, la computadora por la cual se requiere dar respuesta debe responder con su respectiva dirección MAC[54].

Los servidores DNS que responden consultas en modo recursivo son vulnerables a un ataque del tipo de suplantación de respuestas. Algunos emplean la técnica de predicción de secuencia numérica en estos el atacante simula la dirección IP de otra máquina, mientras ataca a otro e intenta la predicción la secuencia numérica seleccionada por el ordenador al que está suplantando[55].

---

[52] Hurtado, Mario. Análisis de Certificados SSL/TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación. En línea. 10 de febrero de 2017. 8 abril de 2020. Disponible en: http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-65422017000100273

[53] Fabian, Buendía. Seguridad informática. Primera edición. Madrid: MCGRAW HILL, 2013. 212p

[54] Ibíd., p.212

[55] Amaro, José. Seguridad en internet. En línea. 2 febrero de 2017. 7 abril de 2020. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072017000100006

Ataque DNS: En este ataque, el servidor DNS es engañado haciéndole creer que está obteniendo una respuesta desde un servidor DNS de confianza. El suplantador realiza una acción que tiene el efecto de modificar la dirección IP de un cierto nombre de dominio por una dirección IP de su propia elección. Una vez que el servidor DNS es engañado se almacena una incorrecta traducción entre un nombre de dominio y una dirección IP, el suplantador puede falsificar las operaciones que se realizan sobre el nombre que ha sido secuestrado[56].

Ataque Wi-fi: Las redes inalámbricas son vulnerables para que se realicen ataques a estas, por lo extendidas en el ámbito personal como empresarial y porque el atacante puede realizar el ataque sin la necesidad de entrar en las instalaciones de la víctima, se puede ingresar situándose cerca para entrar en la cobertura Access Point, consiste en descifrar la contraseña de una conexión en los protocolos WEP, WPA, WPA2 y PIN WPS[57].

El descifrado de contraseñas wifi es el proceso de capturar la contraseña usada como protección de la red wifi. Este tipo de técnicas para decodificar contraseñas se observan a continuación[58]:

Ataques por fuerza bruta: Este tipo de ataque representa el cinco por ciento de las violaciones confirmadas por lo general, implica "adivinar" de cierta manera el nombre de un usuario junto con su contraseña con el fin de obtener acceso no autorizado a un sistema, es un método de ataque simple y usualmente tiene un buen porcentaje de éxito. Se hace uso de aplicativos como herramientas para realizar combinaciones de contraseñas y así poder ingresar al sistema[59].

Monitoreo de la red: se emplea la interceptación de paquetes transmitidos por red, un hacker puede descifrar la contraseña, para esta labor emplea una herramienta denominada Wireshark [60].

---

[56] Herrera, John. Las vulnerabilidades de seguridad de DNS. En línea. 14 febrero de 2018. 5 abril de 2020. Disponible en: https://www.researchgate.net/publication/320985758_Las_vulnerabilidades_de_seguridad_de_DNS

[57] Fabian, Buendía. Seguridad informática. Primera edición. Madrid: MCGRAW HILL, 2013. 214p

[58] Ibíd., p.214

[59] Puig, Toni, Identificación de ataques y técnicas de intrusión. En línea. 27 enero de 2010. 4 de abril de 2020. Disponible en: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/203/A5.pdf?sequence=5

[60] Inteco, Análisis de trafico con wireshark. En línea. 24 de marzo de 2010. 7 de abril de 2020. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

Ataques de denegación de servicio (dos): se clasifica como un ataque de red que tiene como característica una interrupción del servicio de red a los usuarios y los medios tecnológicos. Se clasifican en los siguientes tipos de ataques DoS:

Cantidad abrumadora de tráfico: se origina cuando se realiza un envió de gran cantidad de datos hacia una red, a un host, aplicación o estación de trabajo con una velocidad que supere su gestión. Esto genera que los servicios o dispositivos fallen por la lentitud que genera en la velocidad de transmisión. Paquetes maliciosos formateados**:** esto ocurre cuando se transmite un paquete malicioso formateado a un host o una aplicación y el receptor no puede gestionarlo. Por ejemplo, cuando un hacker realiza el envío de paquetes que tienen errores en las que sus aplicaciones no pueden identificar o reenviar paquetes incorrectamente formateados. Ocasiona que el dispositivo receptor se ejecute con una velocidad no aceptable o se detenga[61].

Los ataques de DoS son un peligro ya que logran detener la comunicación y originar la pérdida valiosa de tiempo y dinero. Son ataques fáciles de realizar [62].

Según ISACA ciberseguridad se define como la "protección de los activos de información al abordar las amenazas de la información procesada, almacenada y transportada por los sistemas de información interconectados"[63].

Estado actual de la ciberseguridad: Actualmente el mundo se encuentra en un cambio constante, la globalización de internet y la tecnología se ha producido a un ritmo ágil, en la que la capacidad de almacenamiento en nuestros dispositivos móviles y computadores que anteriormente no habríamos imaginado y que se encuentran al alcance de nuestra mano, procesadores que constan de más de 8 núcleos, la creación e interconexión de redes de datos han tenido un efecto profundo en nuestro diario vivir, estamos conectados como nunca antes, podemos enviar mensajes de forma instantánea, consultar noticias en tiempo real, etc., pero no todo es perfecto, puesto que siempre existirán vulnerabilidades en las redes y la tecnología, es por ello que hoy en día para muchas empresas la ciberseguridad se convierte en un objetivo fundamental. Mantener segura la información es muy

[61] Voutssas**,** Juan. Preservación documental digital y seguridad informática**.** En línea. 6 de abril de 2010. 10 abril de 2020. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

[62] Diaz, Jairo. Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. En línea. 01 de octubre de 2019. 4 abril de 2020. Disponible en: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872019000200006

[63] Betancourt, Carlos. Ciberseguridad en los sistemas de información de las universidades. 22 agosto 2017. Consultado 12 marzo de 2020. Disponible en: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

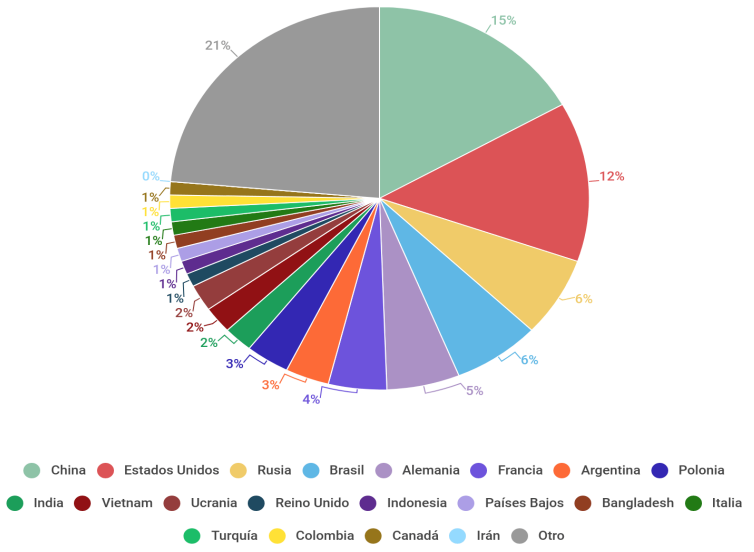
importante, y a medida que la tecnología y las redes avanzan muchas personas se preguntan[64] ¿Cuál es el estado actual de la ciberseguridad?

Ataques de phishing más allá del correo electrónico: No es nada nuevo las estafas en la modalidad de phishing que se realizan a través de los correos electrónicos y páginas web, sin embargo, se ha podido constatar que los teléfonos celulares inteligentes se han convertido en la principal fuente de ataques de phishing, debido a que en los computadores los antivirus cada vez cuentan con un mejor proceso de detección y bloqueo de phishing antes de que perjudique al usuario, caso contrario de lo que sucede en los teléfonos celulares inteligentes[65]. En la figura 12 se encuentran los países víctimas de Phishing para el primer trimestre de 2019.

[64] Calvello, Mara. Tendencias de ciberseguridad para 2020. En línea. 17 de febrero 2020. 20 de marzo de 2020. Disponible en: https://jaxenter.com/cybersecurity-trends-2020-167575.html

[65] Ibíd., p.1

Figura 12. Países con Phishing en el primer trimestre de 2019



Fuente: VERGELIS, Maria, SHCHERBAKOVA, Tatyana, SIDORINA, Tatyana, 15 de mayo de 2019. "Spam and phishing in Q1 2019". Disponible desde Internet en: https://securelist.com/spam-and-phishing-in-q1-2019/90795/

En primer lugar, se encuentra China con un 15,82%, en segundo puesto esta Estados Unidos con 12,64%, en tercer lugar, se ubica Rusia con 6,98%, Brasil en el cuarto puesto 6,95%, y Alemania con un 5,86%, estos son los países más atacados por la modalidad de phishing[66].

[66] Vergelis, Maria. Spam y phishing en el tercer trimestre de 2019. En línea. 26 noviembre de 2019. Consultado 20 marzo de 2020. Disponible en: https://securelist.lat/spam-report-q3-2019/89777/.

ISO 27005: La norma ISO 27005 proporciona directrices con el fin de poder gestionar los riesgos inherentes a la seguridad de la información, se encuentra diseñada para poder implementar de manera correcta la seguridad de la información basada en la orientación de la gestión de los riesgos.

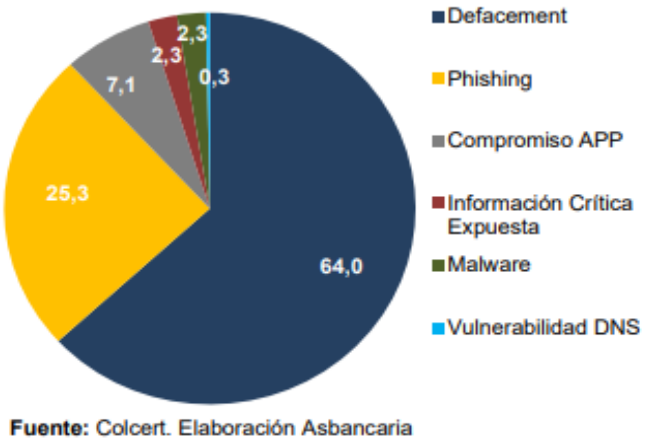
La presente norma se utiliza para todos los tipos de empresas, públicas, privadas, organizaciones sin fines de lucro, que quieran gestionar los riesgos que puedan complicar la seguridad de la información[67].

Según la organización colCERT se presentaron los siguientes datos sobre los tipos de ataques cibernéticos en Colombia en el año 2017. Según la figura 13 se evidencia que el ataque más frecuente es el defacement con el 64%, seguido del phishing con el 25.3 %, y el tipo de ataque menos frecuente es la vulnerabilidad DNS[68].

[67] Norma Técnica Colombiana NTC-ISO/IEC 27005, p.1

[68] Santiago, Castro. En línea. La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones. 23 de abril de 2018. Consultado el 20 marzo 2020.Disponible en: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

Figura 13. Tipos de incidentes cibernéticos en Colombia

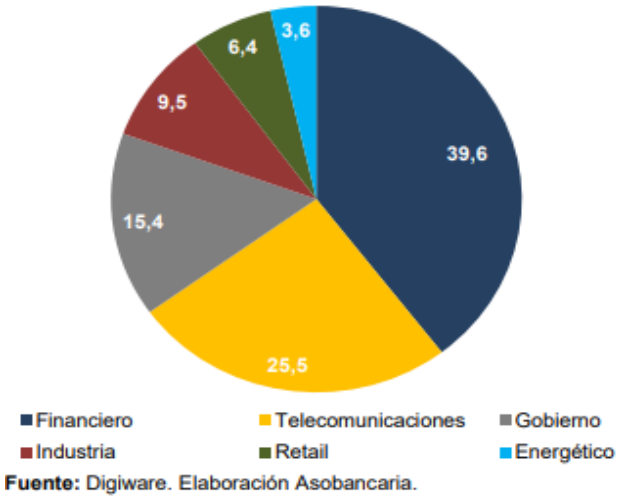


Fuente: ASOBANCARIA, 23 de abril de 2018. "La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones". Disponible desde Internet en: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

Según Digiware en 2017, informo que con respecto a los sectores económicos el sector financiero es el más atacado con 214.000 ataques por día 39,6%, seguido de las telecomunicaciones con el 25.5% con 138.329 ataques por día correspondiente al 25,50% y el gobierno sigue con el 15,4%. Según la figura 14, lo que indica que estos sectores económicos necesitan tener una mayor ciberseguridad frente a los cibercriminales que tienen como predilecto estos rubros[69].

[69] Ibíd., p.4.

Figura 14. Distribución de los ataques cibernéticos por sectores económicos



Fuente: ASOBANCARIA, 23 de abril de 2018. "La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones". Disponible desde Internet en: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

Las nuevas TIC se imponen en todas las áreas de la vida diaria en el que se origina como regla y no excepción el que ciertos comportamientos delictivos tengan lugar en dichas ramas.

En Colombia se establece el documento CONPES 3701 en el cual se especifican directrices nacionales de ciberseguridad y en el que busca contrarrestar el aumento de amenazas informáticas que afectan directamente al país[70].

Según el CONPES, ciberseguridad es la capacidad que tiene el estado para reducir el nivel de riesgo al que están expuestos los ciudadanos ante incidentes cibernéticos[71].

Por ejemplo, según la empresa estadounidense Fortinet, público un estudio en el último congreso de ciberseguridad conocido como andicom que se lleva a cabo en la ciudad de Cartagena, en el cual se reportó que, entre abril y julio del año 2019, Colombia fue objetivo de más de 40 billones de intentos de ciberataques, la empresa Fortinet dio a conocer que la mayoría de los intentos de ciberataques son exploits[72].

[70] Mintic, Ciberseguridad. En linea, 26 diciembre 2019. Consultado 12 marzo de 2020 disponible en: https://www.mintic.gov.co/portal/inicio/Micrositios/I+D+I/Nodos/6120:Ciberseguridad
[71] Ibíd., p.1
[72] Dinero, Ciberseguridad, web,12 marzo de 2019. Consultado 14 marzo de 2020 disponible: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

Los atacantes han desarrollado sus técnicas para conseguir el beneficio económico y esto ha facilitado su labor:

1. Son expertos que descubren nuevas vulnerabilidades no conocidas, denominadas vulnerabilidades de día 0, de las cuales pueden beneficiarse vendiéndolas a los fabricantes o en el mercado negro como la deep web. Utilizan técnicas de ingeniería social para lograr sus fines.

2. Ser parte de una Botnet, el sistema atacado pasa a ser parte de una red de ordenadores controlados remotamente por un atacante el cual los programa para realizar actividades ilícitas como él envió de correo basura a millones de destinatarios.

3. Ser víctima del ataque denominado ransomware en el que la atacante cifra los archivos exigiendo un rescate económico.

4. APTs (amenazas persistentes y avanzadas) combinación de técnicas de ataque, que incluyen diferentes tipos de vulnerabilidades con técnicas de ingeniería social diseñadas para atacar una organización.

5. Ataques de infraestructura critica cuando tienen motivaciones políticas, militares o terroristas, intentan desestabilizar vulnerando sistemas de control en las infraestructuras.

Crimen como servicio en el cual terceras partes desarrollan ciberataques, este consiste en el secuestro del ordenador en el que la víctima queda impotente ante la situación que lo imposibilita a la utilización del mismo, y el cryptoware como una variante de la modalidad de secuestro que implica un cifrado de archivos y en el que ofrecen la promesa de liberar el ordenador mediante un pago de una cifra de dinero determinada[73].

Se utiliza el ciberespacio para desarrollar otras formas de delito en el cual se descubren contrataciones de servicio de grupo de hackers por parte de organizaciones de narcotráfico[74].

[73] Joyanes, Luis. Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial. 4 edición. Madrid: Alfaomega, 2017, 32 p.
[74] Ibíd., p.32

Según el informe anual de seguridad nacional 2014, destaca cinco tipos de ataques:

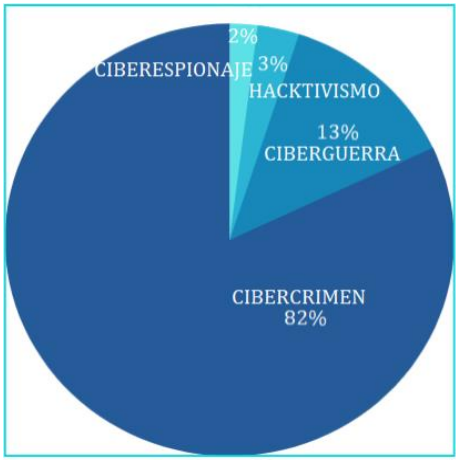
El ciber-espionaje: una de las mayores preocupaciones durante el año 2014 para los gobiernos occidentales[75].
La ciber-delincuencia: durante 2013 los criminales han incrementado la frecuencia, variedad y amplitud de ataques a cambio de una recompensa[76].

El ciber-terrorismo: en sus dos enfoques, uno como instrumento facilitador de sus actividades o como objeto de su acción para la comisión de actividades terroristas[77].

Hacktivismo: engloba aquellos ataques dirigidos por grupos que se caracterizan por una determinada ideología y que buscan atacar la seguridad de los sistemas y la información[78].

La ciber-guerra, que se orienta a realizar operaciones militares y otras que se enfocan a negar, modificar, llevar a engaño o destruir las capacidades propias en los sistemas de información y telecomunicaciones que impactan a la defensa nacional[79]. En la figura 15 se observan las motivaciones encontradas detrás de los ciberataques a nivel mundial en el 2018.

Figura 155. Motivaciones detrás de ciberataques a escala global (2018)



Fuente: URVIO Revista Latinoamericana de Estudios de Seguridad, diciembre de 2019. "Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad". Disponible desde Internet en: http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-42992019000200024

[75] Ibíd., p.32
[76] Ibíd., p.32
[77] Ibíd., p.32
[78] Ibíd., p.32
[79] Ibíd., p.32

3. MARCO JURÍDICO

Se denomina delito electrónico, a la acción que estipule un acceso abusivo a un sistema informático, obstaculización ilegitima de sistema informático o red, interceptación de datos informáticos, uso de software malicioso, violación de datos personales y suplantación de sitios web como se define en la Ley 1273 de 2009 [80].

Acceso abusivo a un sistema informático, se define como el acceso sin autorización a las personas que sin un acuerdo pactado acceda a todo o en parte a un sistema informático protegido o sin ninguna medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y con una multa de 100 a 1.000 salarios mínimos legales mensuales vigentes como se define en el artículo 269A [81].

Obstrucción ilegítima de sistema informático o red de telecomunicación se define a la persona o grupo que impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, como se define en el artículo 269B[82].

Interceptación de datos informáticos, estipula las personas que sin previo permiso realice interceptación de datos informáticos en su origen, destino o en el interior de un sistema informático, artículo 269C: [83].

Daño Informático, se define las personas que dañe, elimine, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes según el artículo 269D [84].

---

[80] Diario oficial, Ley 1273 de 2009. En línea. 5 enero de 2009. 17 marzo 2020. Disponible en: https://www.armada.mil.co/sites/default/files/normograma_arc/telematica/Ley%201273%20de%202009%20Modifica%20CP%20para%20protecci%C3%B3n%20de%20datos%20e%20informaci%C3%B3n.pdf

[81] Congreso de Colombia, En línea. 5 enero de 2009. 18 marzo 2020. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

[82] Ibíd., p.1

[83] Ibíd., p.1

[84] Ibíd., Congreso de Colombia. En línea. 5 enero de 2009. 18 marzo 2020. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Uso de software malicioso estipula que cualquier persona sin autorización que produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación, artículo 269E [85].

Violación de datos personales estipula que cualquier persona sin estar avalado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, según el artículo 269F [86].

Suplantación de sitios web para obtener datos personales, se estipula que una persona sin estar avalado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe, envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave según el artículo 269G [87].

Regulación de transparencia donde se tipifica que toda entidad pública debe publicar información sobre sus activos y procesos que se llevan a cabo en la entidad de manera transparente para la ciudadanía, según la ley 1712 de 2014[88].

Protección de datos personales que regula la protección del derecho fundamental que tienen las personas naturales a autorizar información personal que es almacenada en base de datos o archivos para posteriormente su autorización y rectificación, según la ley 1581 de 2012[89].

Regulación del habeas data y el manejo de la información, según la ley 1266 de 2008[90].

---

[85] Ibíd., p.1
[86] Ibíd., p.1
[87] Ibíd., p.1

[88] María, Hoyos. Decreto 000103. En línea. enero 20 de 2015. Abril 25 de 2020. Disponible en: www-leyex-info.ucatolica.basesdedatosezproxy.com/documents/leyes/Decreto103de2015.pdf

[89] Molano, diego. Ley 1581 de 2012. En línea. 17 octubre de 2012. 25 abril de 2020. Disponible en: https://ucatolica-leyex-info.ucatolica.basesdedatosezproxy.com/normativa/detalle/ley-1581-de-2012-24760/pdf

[90] Cifuentes, Carlos. El debido proceso en la ley del habeas data. En línea. 21 abril de 2017. 25 abril de 2020. Disponible en: http://www.scielo.org.co/pdf/cesd/v8n1/v8n1a11.pdf

4. ESTADO DEL ARTE

Se realiza un estudio de los conceptos de ciberseguridad, ciberguerra, ciberespacio, las diferentes ciber amenazas presentes, así como también las ciberdefensas que los países crean para evitar o reducir los diferentes ataques cibernéticos, así como las medidas que está creando Colombia para estar lo menos expuesta posible en materia de ciberataques como es el caso del CONPES, que entre sus principales objetivos correspondientes a su Política se recalcan los de fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país, y actualizar el marco de gobernanza.

El entorno digital es un escenario donde se desarrollan todo tipo de actividades y, según el Foro Económico Mundial, sin confianza digital es imposible intercambiar bienes o servicios online, debido a esto es de suma importancia para un país como Colombia que se fortalezca la confianza y seguridad digital.

Se da a conocer el estado actual de la ciberseguridad desde el ámbito de las empresas y organizaciones.[91]

Ciberguerra: la ciberguerra puede catalogarse como una agresión impulsada por un estado que busca desprestigiar a otro por intereses propios con el fin de sacar información confidencial, interrumpir o dañar los sistemas de comunicación, modificar sus servidores y extraer data de las bases de datos, es decir, busca incitar a una guerra pero virtual que busca tener acceso a los sistemas informáticos para obtener información hasta el control de proyectiles mediante computadoras, pasando por la planificación de las operaciones, la administración del abastecimiento, etc. [92].

Mediante los medios de comunicación, se han evidenciado los ciberataques dirigidos a organizaciones, empresas, fábricas de diferente índole, ciudadanos, e incluso centrales nucleares [93].

---

[91] Joyanes, Luis. Introducción estado del arte de la ciberseguridad. En línea. 1 Julio de 2010. 18 marzo de 2020. Disponible en: https://dialnet.unirioja.es/descarga/articulo/3837217.pdf

92 Gema, Sánchez. Los estados y la ciberguerra. En línea. 23 octubre 2017. 20 de abril de 2020 Disponible en: https://es.scribd.com/document/362322056/Dialnet-LosEstadosYLaCiberguerra-3745519

[93] Joyanes, Luis. Estado del arte de la ciberseguridad. En línea. 1 julio de 2010. 19 de abril de 2020. Disponible en: Dialnet-IntroduccionEstadoDelArteDeLaCiberseguridad-3837217%20(3).pdf

Se ha realizado una recopilación de ataques relacionadas con la ciberseguridad y ciberguerra en el mundo representadas en la figura 16.

Figura 16. Línea de tiempo de ciberataques en el mundo

Fuente: Elaboración Propia, 2020

Ejército de brasil y la empresa española de seguridad panda security luchan juntos contra la ciberguerra: la empresa Panda Security firmo un acuerdo para el mes de octubre de 2010 con el ejército de Brasil con el fin de apoyar la institución en la profesionalización de sus capacidades operacionales en la lucha contra el ciberterrorismo[94].

El país de Irán fue víctima de varios ataques informáticos: Irán sufrió para el 27 septiembre de 2010 el ataque cibernético más grande de la actualidad, los sistemas de control de la central nuclear en Irán, como también en otras industrias se vieron gravemente afectados por un virus que se conoce como Stuxnet, el cual tiene la capacidad de convertirse en un agente durmiente y poder accionarse a distancia en el momento que su propietario lo requiera sin que el usuario final del equipo se percate[95].

Israel militariza la cibernética: en el país de Israel se cree que el virus denominado Stuxnet el cual ataco centrales nucleares iraníes fue interpuesto por un extranjero quien se limitó a hacer uso de una memoria tipo lápiz electrónico USB que estaba listo para infectar la red iraní, a raíz de esta situación Israel tomo la decisión como lo hicieron y lo están haciendo varias empresas de reclutar a los más grandes expertos en ciberseguridad para así evitar o reducir incidentes en este tema[96].

---

[94] Ibíd.,15

[95] Ibíd.,16

[96] Ibíd.,17.

La unión europea prueba sus defensas en un simulacro de ciberataque: el primer ejercicio de simulación de un ciberataque llevado a cabo en diferentes países de la unión europea dio lugar el 4 de noviembre de 2010 con el fin de mejorar la ciber seguridad frente a los ciberataques. El ejercicio fue denominado "Cyber-Europe 2010" fue organizado por los diferentes países de la unión europea con el apoyo de ENISA (Agencia Europea de seguridad de las redes y de la información). En este ejercicio se expuso a más de 320 incidentes y se tenía como objetivo fortalecer la ciberdefensa en Europa[97].

Piratean la página Web de la Marina Británica: según el medio de comunicación BBC un hacker conocido como TinKode utilizo un método de inyección SQL, un ataque que hace uso de código SQL para extraer información de la página, al darse cuenta de este hecho se suspendió temporalmente la página web de la marina británica. Esta información se dio a conocer el 8 de noviembre de 2010[98].

Supermercado target en Estados Unidos: en el año 2013, se realiza el mayor ataque a target en el que se desvelaron datos sensibles de sus clientes como tarjetas de crédito, correos, direcciones físicas y contraseñas[99].

Ataque cibernético a yahoo afecta 3000 millones de cuentas: en el año 2013, se realiza un ataque cibernético a YAHOO revelando 3000 millones de cuentas activas con datos personales de los usuarios[100]**.**

Ciberataque banco JP Morgan: en el año 2014 se registró el mayor ciberataque de la historia a una entidad financiera. Fue a uno de los mejores bancos de América, JP Morgan Chase, cuando en una operación coordinada se sospechó llegó desde Rusia, los hackers accedieron a 90 servidores de la compañía y comprometieron datos personales y financieros sensibles de 77 millones de clientes y 7 millones de empresas. El hackeo a domino's pizza o la publicación de millones de cuentas y contraseñas de gmail, fueron otros de los sucesos destacados, además de los ataques al sector de la salud, un fenómeno en crecimiento por los beneficios que supone vender registros médicos robados[101].

Ataque a la empresa apple: en septiembre de 2015, Apple experimento uno de los ataques informáticos más importantes de la historia, género que se

---

[97] Ibíd.,18.

[98] Ibíd.,20.

[99] CCN-CERT, Ciber amenazas 2013 y tendencias 2014. En línea. 20 de octubre de 2014. 4 abril de 2020. Disponible en: www.ccn-cert.cni.es/publico/dmpublidocuments/CCN-CERT_IA-03-14-Ciberamenazas_2013_Tendencias_2014-publico.pdf

[100] CNN, Yahoo sufre un ataque cibernético masivo que compromete cuentas de correo. En línea. 31 enero de 2014. 12 abril de 2020. Disponible en: https://cnnespanol.cnn.com/2014/01/31/yahoo-sufre-un-ataque-cibernetico-masivo-que-compromete-cuentas-de-correo/

[101] Clavijo, Felipe. Riesgo cibernético. En línea. 2 julio de 2017. 25 marzo de 2020. Disponible en: https://www.banrep.gov.co/sites/default/files/publicaciones/archivos/rref_recuadro_7_2017.pdf

desinstalara más de cincuenta aplicaciones que contenían malware y que pretendían hurtar datos de los dispositivos de los usuarios. Para este año Sony Pictures Entertainment quedó paralizado por la intrusión de un grupo de hackers que robaron más de 33.000 documentos con información expuesta de la compañía y sus empleados[102].

Ataque botnet a infraestructura dyn: en octubre del año 2016 se realizó un ataque llevado a cabo por una red de robots o botnet Mirai, que infecto dispositivos del internet de las Cosas (IoT) por ejemplo cámaras IP y routers domésticos, compuesto por una red de dispositivos zombis. Este ataque masivo sobre denegación de servicio distribuido (DDoS) contra la infraestructura de DNS del proveedor de infraestructura Dyn, afecto a usuarios de empresas tan relevantes como Twitter, Amazon, Tumblr, Reddit, Spotify, Paypal y Netflix, bloqueando el acceso a los servicios[103].

Elecciones presidenciales en Estados Unidos: en el año 2016, hackers informáticos filtraron miles de correos electrónicos del Comité Nacional Demócrata (DNC), en el transcurso de las elecciones presidenciales de 2016, al realizar infiltración de correos en las campañas. El departamento de justicia de Estados Unidos acusó más tarde a 12 rusos que eran agentes de la agencia de inteligencia militar de Rusia, el GRU por llevar a cabo el ataque cibernético[104].

Ransomware en el mundo: en el año 2017, se evidenciaron múltiples ataques, sofisticados, potentes y con mayor alcance e impacto a lo largo del mundo. Dentro de los incidentes cibernéticos más importantes se encuentra el ransomware “WannaCry”, que afectó más de 360.000 dispositivos en más de 180 países y generó a sus fundadores más de USD 100.000 dólares en rescates[105].

Ataque bundestag alemán: en enero de 2019, la Oficina Federal de Seguridad de la Información de Alemania investigo un ataque cibernético contra cientos de políticos, incluida la canciller alemana, Angela Merkel. El ataque cibernético se orientó a todos los partidos en el parlamento alemán. Información financiera, tarjetas de identificación y chats privados se encontraban entre los datos que los piratas informáticos publicaron en la red. Números de fax, direcciones de correo electrónico y varias de sus cartas fueron publicadas[106].

---

[102] Joyanes, Luis. Ciberseguridad. En línea. 1 septiembre de 2015. 12 de abril de 2020. Disponible en: Dialnet-Ciberseguridad-6115620%20(2).pdf

[103] Pollard, Jeff, Botnet Mirai. En línea. 24 octubre de 2016. 20 de abril de 2020. Disponible en: https://www.akamai.com/es/es/multimedia/documents/white-paper/akamai-mirai-botnet-and-attacks-against-dns-servers-white-paper.pdf

[104] Actualidad, Seis ataques cibernéticos que sacudieron al mundo. En linea.5 enero de 2019. Disponible en: https://www.dw.com/es/seis-ataques-cibern%C3%A9ticos-que-sacudieron-el-mundo/a-46967214

[105] Ibíd., p.1

[106] Ibíd., p.1

Grandes avances de la ciberseguridad: entre los más grandes avances de la ciberseguridad los más destacados son relacionados a continuación.

Machine learning y Deep learning: El machine learning o aprendizaje automático hace parte de la inteligencia artificial, este consiste en que las maquinas aprendan sin la necesidad de una previa programación, con esto los sistemas se vuelven más autónomos, hábiles y tener la capacidad de identificar patrones obtenidos de datos con el fin de realizar pronósticos. Machine learning se encuentra presenta en muchas aplicaciones actualmente como, por ejemplo, Netflix, Spotify, los asistentes de celulares Siri y Alexa, etcétera[107].
El Deep learning también conocido como aprendizaje profundo se trata de un algoritmo automatizado organizado, pertenece a un subcampo de Machine learning, el Deep learning simula el aprendizaje de las personas con el propósito de obtener conocimientos. Este algoritmo sobresale por estar compuesto por redes neuronales conectadas para el procesamiento de datos, los algoritmos que hacen parte de un sistema de aprendizaje profundo o Deep learning se encuentran en 3 diferentes capas neuronales las cuales son:

- Capa de entrada, aquí se asimilan los datos de entrada como por ejemplo una tabla de datos.
- Capa oculta, aquí se encuentra la red que ejecuta el procesamiento de la información y se realizan los cálculos intermedios.
- Capa de salida, aquí se encuentra la red que toma la decisión o en su lugar genera alguna conclusión contribuyendo de esta manera a los datos de salida.[108].

El malware ha crecido en una gran cantidad en los últimos años, generando perdidas a muchas organizaciones, diferentes empresas antimalware han propuesto diferentes alternativas para defenderse de los ataques con malware, la complejidad, velocidad y complejidad representan nuevos desafíos para la comunidad en contra del malware. Las empresas antimalware junto con investigadores emprendieron el uso de métodos de machine learning y Deep learning para el análisis y detección de malware[109]. Una de las empresas antimalware más reconocidas a nivel mundial, implemento la tecnología Deep learning, dicha empresa es Sophos, entre las principales características más relevantes que trae el uso de esta tecnología encontramos, evitar el malware conocido y desconocido hasta la fecha, no depender de firmas como la gran mayoría de antivirus lo hacen actualmente, ocupar un espacio muy reducido, aproximadamente 20 megas o menos, detectar el malware en 20 milisegundos

[107] BBVA, machine-learning-que-es-y-como-funciona, página web, 08 noviembre 2019, Consultado 30 abril de 2020 disponible en: https://www.bbva.com/es/machine-learning-que-es-y-como-funciona/
[108] Smart Panel, que-es-deep-learning, página web, 10 abril 2020, Consultado 30 abril de 2020 disponible en: https://www.smartpanel.com/que-es-deep-learning/
[109] Arxiv,abs, página web, 04 abril 2019, Consultado 30 abril de 2020 disponible en: https://arxiv.org/abs/1904.02441

aproximadamente, identificar el punto de origen de un ataque, capturar todos los archivos que fueron objetivos de un ataque, revertir los archivos a una versión anterior[110].

[110] infosecurityvip, ISEC InfoSecurity Calo Sophos, página web, 04 abril 2019, Consultado 30 abril de 2020 disponible en: http://www.infosecurityvip.com/newsletter/papers/ISEC%20INFOSECURITY%20CALI%20-%20SOPHOS.PDF

5. METODOLOGÍA

5.1. FASES DEL TRABAJO DE GRADO

Para el desarrollo del presente proyecto, se utilizará una metodología de tratamiento de riesgos basado en la norma 27005, la cual permite efectuar el análisis y valoración de riesgos de los activos de información, cuyas fases se conforman por:

Fase 1 – Establecimiento de contexto[111] Aquí se establece la información más relevante de la entidad con el fin de poder establecer el contexto de la gestión del riesgo en la seguridad de la información.

Fase 2 - Valoración de riesgos[112] Esta fase se encuentra referenciada como proceso en la norma ISO 27001, consta de dos sub fases las cuales son: identificación del riesgo y estimación del riesgo.

Análisis del riesgo: Se compone de la identificación y valoración de los activos y amenazas.

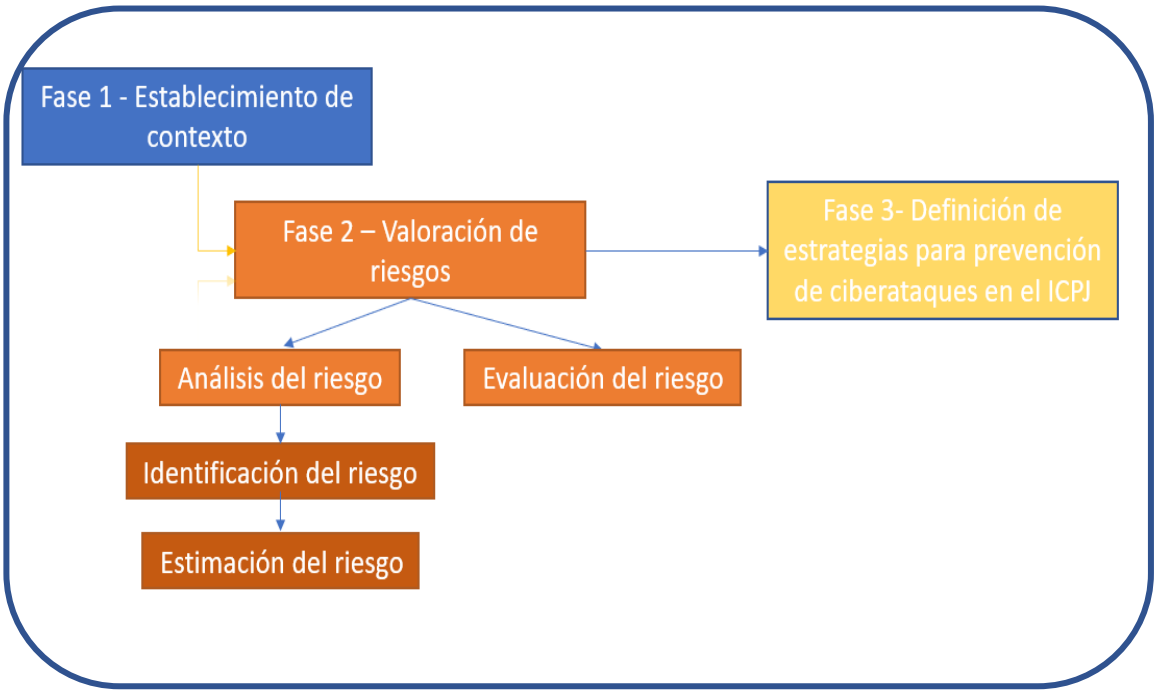
Estimación del riesgo: Se realiza una valoración cualitativa o cuantitativa de los riesgos que afectan los activos de información previamente identificados.

Fase 3 – Definición de estrategias para prevención de ciberataques en el ICPJ: Se definen una serie de estrategias o recomendaciones con el fin de proteger la información crítica de la entidad que se gestiona a través de los activos de información.

[111] Norma Técnica Colombiana NTC-ISO/IEC 27005, Numeral 7, p.7
[112] Ibíd., Numeral 8, p.11

En la figura 17 se encuentra la representación del modelo de la metodología a usar.

Figura 17. Modelo de la metodología



Fuente: ICONTEC, 19 de agosto de 2019. "Norma Técnica Colombiana NTC-ISO/IEC 27005". Disponible desde Internet en: http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001071&ruta=/documentacion/0000001359/0000000107

5.2. INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

NMAP: software libre el cual se emplea para escanear las redes, puertos y debilidades de procesos que sirven como entrada a los sistemas. Utilizado comúnmente en auditorías de seguridad y monitoreo de redes, se utiliza para[113]:

- Identificar los dispositivos conectados a la red que se requiere analizar.
- Identificar los puertos abiertos, el sistema operativo o aplicación en ejecución y su versión.
- Detectar servicios vulnerables en la red.

Nessus: es una potente aplicación de carácter privado que sirve para escanear vulnerabilidades y detectar fallos de seguridad en los sistemas informáticos en base a plugins y módulos que se actualizan periódicamente. Creado por la empresa Tenable, utilizada por expertos en seguridad cibernética cuando tienen que realizar auditorías[114].

Metasploit: Es software libre que se utiliza como framework de ataque para el desarrollo y ejecución de exploits que sirven para vulnerar a una maquina remota[115].

Kali Linux: Es un sistema basado en Linux el cual contiene una cantidad considerable de herramientas preinstaladas con el fin de ayudar con las labores de seguridad de la información[116].

Solarwinds (opcional)

[113] Muñoz, Camilo. Aanálisis de metodologías de ethical hacking para la detección de vulnerabilidades en las pymes. En línea. 24 julio de 2019. 26 abril de 2020 de 2020. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/30302/ccpenagosm.pdf?sequence=1&isAllowed=y

[114] González, María. Protocolo de gestión de vulnerabilidades. En línea. 2 febrero de 2019. 27 abril de 2020. Disponible en: http://bibing.us.es/proyectos/abreproy/92187/fichero/TFG-2187-GONZALEZ.pdf

[115] Gómez, Antonio. Herramientas básicas del hacker. En línea. 2 marzo 2015. 10 abril de 2020. Disponible en: https://ucys.ugr.es/download/taller3/Taller3_Metasploit_Part1.pdf

[116] Educative, what-is-kali-linux, página web, Consultado 15 marzo de 2020 disponible en: https://www.educative.io/edpresso/what-is-kali-linux

5.3. POBLACIÓN Y MUESTRA

El análisis será realizado en la entidad ICPJ tomando como muestra los activos de información críticos para llevar a cabo la misión de la entidad.

5.4. ALCANCES Y LIMITACIONES

1. El proyecto contempla la definición e implementación de estrategias para la prevención de ciberataques que vulneren la información misional del Instituto colombiano para la juventud.

2. El proyecto tiene un tiempo de duración de 4 meses.

3. El área de tecnología del ICPJ implementara las estrategias que se requieran con más urgencia de acuerdo a la criticidad de los activos de información.

6. PRODUCTOS A ENTREGAR

Trabajo de grado

Se realizará un documento de trabajo de grado, con su respectiva entrega al comité académico.

Articulo IEEE

Se creará un artículo científico en formato IEEE de carácter investigativo y su respectiva entrega al comité académico.

7. ENTREGA DE RESULTADOS E IMPACTOS

Fase 1 – Establecimiento de contexto:
Es fundamental determinar el propósito de la gestión del riesgo en la seguridad de la información del ICPJ, en este caso el propósito es la creación de un plan para el tratamiento de riesgos en los activos informáticos a través de los cuales se gestión la información crítica del ICPJ y que pueden estar expuestos a unos niveles de alto riesgo.

Fase 2 – Valoración de riesgos

Análisis del riesgo
Identificación de los activos: Con el fin de proceder con el análisis de riesgos de los activos informáticos que gestionan la información Core de la entidad, primeramente, se realiza la identificación de dichos activos:

Tabla 2. Identificación de activos

TIPO	ID	NOMBRE DEL ACTIVO
SERVICIO	1	Controlador de dominio
	2	Controlador de dominio alterno
	3	Correo electrónico G-SUITE
	4	Portal Institucional
	5	Canal de internet y red MPLS
	6	Acceso a red privada virtual (VPN)
APLICACIONES	7	Sistema de información misional SIM
	8	Software de Sistemas operativos
	9	Software de Base de Datos
	10	Software de Aplicaciones Ofimáticas
	11	Software de gestión documental ORFEO
	12	Software para el control de inventarios
	13	Software para copias de respaldo Veeam Backup
	14	Software de virtualización
	15	Software de acceso biométrico
	16	Antivirus Bitdefender
INFORMACIÓN DIGITAL	17	Copias de respaldo en cintas de la información misional, gestión documental, control de inventarios, portal institucional y servidores.
EQUIPOS	18	Firewall Palo Alto
	19	Servidor Mercurio (Active Directory Principal)
	20	Servidor Venus (Active Directory Secundario)
	21	Servidor Earth (Portal Institucional)
	22	Servidor Marte (Sistema de información misional SIM)

	23	Servidor Jupiter (Software de gestión documental ORFEO)
	24	Servidor Saturno (Control de inventarios)
	25	Servidor Titan (Copias de respaldo Veeam Backup)
	26	Servidor Neptuno (Antivirus Bitdefender)
	27	Servidor de virtualización
	28	Equipos de cómputo
INFRAESTRUCTURA FISICA	29	Lectores biométricos
	30	Datacenter
	31	Switches

Fuente: Área de Tecnología ICPJ

Valoración de activos: A continuación, se realiza una valoración de cada uno de los activos previamente identificados tomando en cuenta las siguientes dimensiones de seguridad:

- (D) Disponibilidad
- (I) Integridad
- (C) Confidencialidad

Y los siguientes criterios de valoración:

Tabla 3. Criterios de valoración

Valor			**Criterio**
MA	Muy alto	9 - 10	Afectación muy severa
A	Alto	6 - 8	Afectación severa
MA	Medio	3 - 5	Afectación intermedia
B	Bajo	1 - 2	Afectación menor
MB	Muy bajo	0	No tiene relevancia

Fuente: Área de Tecnología ICPJ

Anotación: estas valoraciones fueron obtenidas a través de una entrevista a la persona responsable de cada uno de los activos de información.

Tabla 4. Valoración de activos

TIPO	ACTIVO	DIMENSIONES		
		D	I	C
SERVICIO	Controlador de dominio	10	10	10
	Controlador de dominio alterno	10	10	10
	Correo electrónico G-SUITE	5	9	10
	Portal Institucional	5	10	1
	Canal de internet y red MPLS	10	6	10
	Acceso a red privada virtual (VPN)	7	7	10
APLICACIONES	Sistema de información misional SIM	10	10	10
	Software de Sistemas operativos	9	9	4
	Software de Base de Datos	10	10	10
	Software de Aplicaciones Ofimáticas	2	5	2
	Software de gestión documental ORFEO	8	8	8
	Software para el control de inventarios	9	9	8
	Software para copias de respaldo Veeam Backup	9	9	5
	Software de virtualización	9	8	5
	Software de acceso biométrico	5	7	6
	Antivirus Bitdefender	9	8	5
INFORMACIÓN	Copias de respaldo en cintas de la información misional, gestión documental, control de inventarios, portal institucional y servidores.	10	10	5
EQUIPOS	Firewall Palo Alto	9	8	5
	Servidor Mercurio (Active Directory Principal)	8	8	6
	Servidor Venus (Active Directory Secundario)	8	8	6
	Servidor Earth (Portal Institucional)	5	5	6
	Servidor Marte (Sistema de información misional SIM)	10	10	10
	Servidor Jupiter (Software de gestión documental ORFEO)	6	6	6
	Servidor Saturno (Control de inventarios)	8	8	6
	Servidor Titan (Copias de respaldo Veeam Backup)	9	9	6
	Servidor Neptuno (Antivirus Bitdefender)	8	8	5
	Servidor de virtualización	10	10	8
	Equipos de cómputo	7	7	7
INFRAESTRUCTURA FISICA	Lectores biométricos	7	7	7
	Datacenter	8	8	5
	Switches	8	8	5

Fuente: Área de Tecnología ICPJ

Identificación y valoración de amenazas: Una vez realizado el proceso de valoración, se procede a identificar y valorar las amenazas por cada uno de los activos de información, para la identificación de amenazas se utilizará como base la clasificación establecida en la norma ISO 27005, establecida en cuatro grupos:

- Desastres naturales
- Origen industrial
- Equivocaciones y fallas no intencionadas
- Ataques intencionados

Para la probabilidad de ocurrencia de la amenaza, se tomarán los siguientes niveles de probabilidad:

Tabla 5. Criterios de probabilidad

Probabilidad		
Valor	9 - 10	MA
	7 - 8	A
	4 - 6	M
	1 – 3	B
	0	MB

Fuente: El autor

Tabla 6. Identificación y valoración de amenazas tipo: Servicio

ACTIVO	AMENAZAS	PROBABILIDAD
Controlador de dominio	Equivocaciones por parte del administrador del sistema	B
	Modificación de la información	B
	Destrucción de la información	MB
	Fugas de información	B
	Caída del sistema por fallas de energía	MB
	Suplantación de la identidad del usuario	B
	Abuso de privilegios de acceso	M
	Acceso no autorizado	B
Controlador de dominio alterno	Equivocaciones por parte del administrador del sistema	B
	Modificación de la información	B
	Destrucción de la información	MB
	Fugas de información	B
	Caída del sistema por fallas de energía	B
	Suplantación de la identidad del usuario	B
	Abuso de privilegios de acceso	B
	Acceso no autorizado	B
Correo electrónico G-SUITE	Equivocaciones por parte del administrador del sistema	MB
	Modificación de la información	MB
	Destrucción de la información	B
	Fugas de información	B
	Caída del sistema por fallas de energía	MB
	Suplantación de la identidad del usuario	MB
	Abuso de privilegios de acceso	MB
	Acceso no autorizado	B
	Errores por parte de los usuarios	B
Portal Institucional	Equivocaciones por parte del administrador del sistema	MB
	Modificación de la información	B
	Destrucción de la información	B
	Fugas de información	MB
	Caída del sistema por fallas de energía	MB
	Suplantación de la identidad del usuario	MB
	Abuso de privilegios de acceso	M
	Acceso no autorizado	B
	Errores por parte de los usuarios	B
	Errores de monitorización (log)	B

	Errores de configuración	B
	Vulnerabilidades en la página web	M
	Errores de mantenimiento	M
	Caída del sistema por fallas de energía	MB
	Intrusión de código malicioso	B
	Denegación de servicio	B
Canal de internet y red MPLS	Fuego	B
	Daños por agua	MB
	Desastres naturales	B
	Avería de origen físico o lógico	B
	Caída del sistema por fallas de energía	B
	Condiciones inadecuadas de temperatura o humedad	B
	Interrupción deliberada por un agente externo	B
	Errores de configuración	MB
	Errores de mantenimiento / actualización de equipos (hardware)	B
	Robo de equipos	B
Acceso a red privada virtual (VPN)	Equivocaciones por parte del administrador del sistema	B
	Fugas de información	B
	Suplantación de la identidad del usuario	M
	Abuso de privilegios de acceso	MB
	Acceso no autorizado	B
	Errores por parte de los usuarios	B

Fuente: Área de Tecnología ICPJ

Tabla 7. Identificación y valoración de amenazas tipo: Aplicaciones

ACTIVO	AMENAZAS	PROBABILIDAD
Sistema de información misional SIM	Errores por parte de los usuarios	B
	Equivocaciones por parte del administrador del sistema	B
	Errores de monitorización (log)	B
	Errores de configuración	B
	Modificación de la información	B
	Errores de mantenimiento	M
	Caída del sistema por fallas de energía	B
	Intrusión de código malicioso	M
	Denegación de servicio	M
Software de Sistemas operativos	Errores por parte de los usuarios	B
	Equivocaciones por parte del administrador del sistema	MB
	Errores de monitorización (log)	B
	Errores de configuración	B
	Modificación de la información	B
	Errores de mantenimiento	B
	Caída del sistema por fallas de energía	B
	Intrusión de código malicioso	M
Software de Base de Datos	Equivocaciones por parte del administrador del sistema	B
	Errores de monitorización (log)	B
	Errores de configuración	B
	Modificación de la información	B
	Errores de mantenimiento	B
	Caída del sistema por fallas de energía	B
	Intrusión de código malicioso	B
Software de Aplicaciones Ofimáticas	Errores por parte de los usuarios	B
	Errores de configuración	B
	Modificación de la información	B
	Errores de mantenimiento	B
	Intrusión de código malicioso	B
Software de gestión documental ORFEO	Errores por parte de los usuarios	B
	Equivocaciones por parte del administrador del sistema	B
	Errores de monitorización (log)	B
	Errores de configuración	B
	Modificación de la información	B

	Errores de mantenimiento	M
	Caída del sistema por fallas de energía	B
	Intrusión de código malicioso	MB
Software para el control de inventarios	Errores por parte de los usuarios	B
	Equivocaciones por parte del administrador del sistema	B
	Errores de monitorización (log)	B
	Errores de configuración	B
	Modificación de la información	B
	Errores de mantenimiento	B
	Caída del sistema por fallas de energía	B
	Intrusión de código malicioso	M
	Denegación de servicio	M
Software para copias de respaldo Veeam Backup	Equivocaciones por parte del administrador del sistema	B
	Errores de monitorización (log)	B
	Errores de configuración	B
	Modificación de la información	B
	Errores de mantenimiento	M
	Caída del sistema por fallas de energía	B
	Intrusión de código malicioso	B
Software de virtualización	Equivocaciones por parte del administrador del sistema	B
	Errores de monitorización (log)	B
	Errores de configuración	B
	Modificación de la información	B
	Errores de mantenimiento	M
	Caída del sistema por fallas de energía	B
	Intrusión de código malicioso	B
Software de acceso biométrico	Errores por parte de los usuarios	MB
	Equivocaciones por parte del administrador del sistema	MB
	Errores de monitorización (log)	B
	Errores de configuración	B
	Modificación de la información	B
	Errores de mantenimiento	MB
	Caída del sistema por fallas de energía	M
	Intrusión de código malicioso	MB
	Denegación de servicio	MB
Antivirus Bitdefender	Errores por parte de los usuarios	B
	Equivocaciones por parte del administrador del sistema	MB
	Errores de monitorización (log)	B

	Errores de configuración	B
	Modificación de la información	B
	Caída del sistema por fallas de energía	MB
	Errores de mantenimiento	B
	Abuso de privilegios de acceso	B

Fuente: Área de Tecnología ICPJ

Tabla 8. Identificación y valoración de amenazas tipo: Información

ACTIVO	AMENAZAS	PROBABILIDAD
Información digital	Errores de configuración	B
	Errores de monitorización (log)	B
	Alteración de la información	B
	Errores de mantenimiento	B
	Intrusión de código malicioso	B

Fuente: Área de Tecnología ICPJ

Tabla 9. Identificación y valoración de amenazas tipo: Equipos

ACTIVO	AMENAZAS	PROBABILIDAD
Firewall Palo Alto	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	B
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	MB
	Acceso no autorizado	B
Servidor Mercurio (Active Directory Principal)	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	B
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	MB
	Acceso no autorizado	B
Servidor Venus (Active Directory Secundario)	Fuego	B
	Daños por agua	B
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	B
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	MB
	Acceso no autorizado	B
Servidor Earth (Portal Institucional)	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	B

	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	MB
	Acceso no autorizado	B
Servidor Marte (Sistema de información misional SIM)	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	B
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	MB
	Acceso no autorizado	B
Servidor Jupiter (Software de gestión documental ORFEO)	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	B
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	MB
	Acceso no autorizado	B
Servidor Saturno (Control de inventarios)	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	B
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	MB
	Acceso no autorizado	B
Servidor Titan (Copias de respaldo	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB

Veeam Backup)	Caída del sistema por fallas de energía	B
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	MB
	Acceso no autorizado	B
Servidor Neptuno (Antivirus Bitdefender)	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	B
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	MB
	Acceso no autorizado	B
Servidor de virtualización	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	B
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	MB
	Acceso no autorizado	B
Equipos de cómputo	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	B
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	M
	Acceso no autorizado	B

Fuente: Área de Tecnología ICPJ

Tabla 10. Identificación y valoración de amenazas tipo: Infraestructura física

ACTIVO	AMENAZAS	PROBABILIDAD
Lectores biométricos	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	M
	Condiciones de temperatura no aptas	B
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	MB
	Acceso no autorizado	MB
Datacenter	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	B
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	B
	Robo de equipos	MB
	Acceso no autorizado	B
Switches	Fuego	B
	Daños por agua	M
	Desastres naturales	B
	Desastres industriales	MB
	Caída del sistema por fallas de energía	M
	Condiciones de temperatura no aptas	M
	Equivocaciones por parte del administrador del sistema	B
	Errores de mantenimiento	M
	Robo de equipos	M
	Acceso no autorizado	B

Fuente: Área de Tecnología ICPJ

Estimación del riesgo

Impacto potencial: Primero de debe realizar una valoración cualitativa para conocer la magnitud del impacto de las amenazas que llegase a materializarse sobre los activos identificados previamente.

Valoración considerada para el impacto

Tabla 11. Criterios de impacto

Impacto		
Valor	9 - 10	MA
	7 - 8	A
	4 - 6	M
	1 – 3	B
	0	MB

Fuente: Área de Tecnología ICPJ

Tabla 12. Impacto para la categoría: Servicios

ACTIVO	AMENAZAS	DIMENSIONES		
		D	I	C
Controlador de dominio	Equivocaciones por parte del administrador del sistema	A	A	A
	Modificación de la información	MB	MA	MA
	Destrucción de la información	MA	MA	MA
	Fugas de información	M	MA	M
	Caída del sistema por fallas de energía	A	MB	MB
	Suplantación de la identidad del usuario	MB	A	A
	Abuso de privilegios de acceso	MB	A	A
	Acceso no autorizado	MB	A	A
Controlador de dominio alterno	Equivocaciones por parte del administrador del sistema	A	A	A
	Modificación de la información	MB	MA	MA
	Destrucción de la información	MA	MA	MA
	Fugas de información	M	MA	M
	Caída del sistema por fallas de energía	A	MB	MB
	Suplantación de la identidad del usuario	MB	A	A
	Abuso de privilegios de acceso	MB	A	A
	Acceso no autorizado	MB	A	A
Correo electrónico G-SUITE	Equivocaciones por parte del administrador del sistema	MB	MB	MB
	Modificación de la información	MB	MB	MB
	Destrucción de la información	B	B	MB
	Fugas de información	MB	MB	B
	Caída del sistema por fallas de energía	MB	MB	MB
	Suplantación de la identidad del usuario	MB	MB	MB
	Abuso de privilegios de acceso	MB	B	B
	Acceso no autorizado	MB	MB	MB
	Errores por parte de los usuarios	MB	B	B
Portal Institucional	Equivocaciones por parte del administrador del sistema	A	A	MB
	Modificación de la información	MB	A	MB
	Destrucción de la información	MB	A	MB
	Fugas de información	MB	A	MB
	Caída del sistema por fallas de energía	MA	MA	MB
	Suplantación de la identidad del usuario	A	A	MB
	Abuso de privilegios de acceso	M	M	MB
	Acceso no autorizado	A	A	MB
	Errores por parte de los usuarios	MB	MB	MB
	Errores de monitorización (log)	B	B	MB

	Errores de configuración	A	A	MB
	Vulnerabilidades en la página web	A	A	MB
	Errores de mantenimiento	M	M	MB
	Caída del sistema por fallas de energía	MB	MB	MB
	Intrusión de código malicioso	M	M	MB
	Denegación de servicio	B	MB	MB
Canal de internet y red MPLS	Fuego	MA	MB	MB
	Daños por agua	MA	MB	MB
	Desastres naturales	MA	MB	MB
	Avería de origen físico o lógico	MA	MB	MB
	Caída del sistema por fallas de energía	A	MB	MB
	Condiciones inadecuadas de temperatura o humedad	A	MB	MB
	Interrupción deliberada por un agente externo	A	MB	MB
	Errores de configuración	A	MB	MB
	Errores de mantenimiento / actualización de equipos (hardware)	A	MB	MB
	Robo de equipos	MA	MB	MB
Acceso a red privada virtual (VPN)	Equivocaciones por parte del administrador del sistema	A	MB	MB
	Fugas de información	M	MB	MB
	Suplantación de la identidad del usuario	M	MB	MB
	Abuso de privilegios de acceso	A	MB	MB
	Acceso no autorizado	A	MB	MB
	Errores por parte de los usuarios	MB	MB	MB

Fuente: Área de Tecnología ICPJ

Tabla 13. Impacto para la categoría: Aplicaciones

ACTIVO	AMENAZAS	DIMENSIONES		
		D	I	C
Sistema de información misional SIM	Errores por parte de los usuarios	MB	MB	MB
	Equivocaciones por parte del administrador del sistema	MA	MA	MA
	Errores de monitorización (log)	MB	MB	MB
	Errores de configuración	MA	MA	MA
	Modificación de la información	MB	MA	MA
	Errores de mantenimiento	A	A	MB
	Caída del sistema por fallas de energía	MA	MB	MB
	Intrusión de código malicioso	MA	MA	MA
	Denegación de servicio	MA	MB	MB
Software de Sistemas operativos	Errores por parte de los usuarios	B	MB	MB
	Equivocaciones por parte del administrador del sistema	A	A	MB
	Errores de monitorización (log)	MB	MB	MB
	Errores de configuración	M	MB	MB
	Modificación de la información	B	MB	MB
	Errores de mantenimiento	MA	MA	MB
	Caída del sistema por fallas de energía	MA	MB	MB
	Intrusión de código malicioso	MA	MA	MA
Software de Base de Datos	Equivocaciones por parte del administrador del sistema	MA	M	MB
	Errores de monitorización (log)	MB	MB	MB
	Errores de configuración	M	M	MB
	Modificación de la información	B	MA	MB
	Errores de mantenimiento	A	B	MB
	Caída del sistema por fallas de energía	A	B	MB
	Intrusión de código malicioso	MA	MA	MA
Software de Aplicaciones Ofimáticas	Errores por parte de los usuarios	B	MB	MB
	Errores de configuración	B	MB	MB
	Modificación de la información	A	B	B
	Errores de mantenimiento	M	B	B
	Intrusión de código malicioso	A	A	MB
Software de gestión documental ORFEO	Errores por parte de los usuarios	B	B	A
	Equivocaciones por parte del administrador del sistema	MA	MA	MA
	Errores de monitorización (log)	MB	MB	MB
	Errores de configuración	A	A	A
	Modificación de la información	B	MA	M
	Errores de mantenimiento	A	A	A

	Caída del sistema por fallas de energía	MA	MB	MB
	Intrusión de código malicioso	MA	MA	MA
Software para el control de inventarios	Errores por parte de los usuarios	MB	B	B
	Equivocaciones por parte del administrador del sistema	A	A	A
	Errores de monitorización (log)	MB	MB	MB
	Errores de configuración	A	A	A
	Modificación de la información	MB	MA	B
	Errores de mantenimiento	A	M	MB
	Caída del sistema por fallas de energía	MA	B	MB
	Intrusión de código malicioso	MA	MA	MA
	Denegación de servicio	MA	B	MB
Software para copias de respaldo Veeam Backup	Equivocaciones por parte del administrador del sistema	MA	A	M
	Errores de monitorización (log)	MB	MB	MB
	Errores de configuración	A	A	MB
	Modificación de la información	MB	MA	MB
	Errores de mantenimiento	A	A	MB
	Caída del sistema por fallas de energía	MA	M	MB
	Intrusión de código malicioso	MA	MA	MA
Software de virtualización	Equivocaciones por parte del administrador del sistema	MA	A	M
	Errores de monitorización (log)	MB	MB	MB
	Errores de configuración	A	A	MB
	Modificación de la información	MB	MA	MB
	Errores de mantenimiento	A	A	MB
	Caída del sistema por fallas de energía	MA	M	MB
	Intrusión de código malicioso	MA	MA	MA
Software de acceso biométrico	Errores por parte de los usuarios	MB	MB	MB
	Equivocaciones por parte del administrador del sistema	A	A	MB
	Errores de monitorización (log)	MB	MB	MB
	Errores de configuración	A	A	MB
	Modificación de la información	MB	MA	MB
	Errores de mantenimiento	A	MB	MB
	Caída del sistema por fallas de energía	M	B	MB
	Intrusión de código malicioso	MA	MA	MA
	Denegación de servicio	MA	B	MB
Antivirus Bitdefender	Errores por parte de los usuarios	B	B	B
	Equivocaciones por parte del administrador del sistema	M	B	MB
	Errores de monitorización (log)	MB	MB	MB
	Errores de configuración	M	B	MB

	Modificación de la información	M	B	MB
	Caída del sistema por fallas de energía	B	B	MB
	Errores de mantenimiento	B	B	MB
	Abuso de privilegios de acceso	B	B	MB

Fuente: Área de Tecnología ICPJ

Tabla 14. Impacto para la categoría: Información

ACTIVO	AMENAZAS	DIMENSIONES		
		D	I	C
Información digital	Errores de configuración	B	B	B
	Errores de monitorización (log)	MB	MB	MB
	Alteración de la información	MB	MA	MB
	Errores de mantenimiento	A	M	MB
	Intrusión de código malicioso	M	M	A

Fuente: Área de Tecnología ICPJ

Tabla 15. Impacto para la categoría: Equipos

ACTIVO	AMENAZAS	DIMENSIONES		
		D	I	C
Firewall Palo Alto	Fuego	M	MB	MB
	Daños por agua	M	MB	MB
	Desastres naturales	M	MB	MB
	Desastres industriales	M	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB
	Errores de mantenimiento	MA	MB	MB
	Robo de equipos	MA	MB	MB
	Acceso no autorizado	B	MB	MB
Servidor Mercurio (Active Directory Principal)	Fuego	A	MB	MB
	Daños por agua	A	MB	MB
	Desastres naturales	A	MB	MB
	Desastres industriales	A	MB	MB
	Caída del sistema por fallas de energía	A	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB
	Errores de mantenimiento	M	MB	MB
	Robo de equipos	MA	MB	MB
	Acceso no autorizado	B	MB	MB
Servidor Venus (Active Directory Secundario)	Fuego	A	MB	MB
	Daños por agua	A	MB	MB
	Desastres naturales	A	MB	MB
	Desastres industriales	A	MB	MB
	Caída del sistema por fallas de energía	A	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB
	Errores de mantenimiento	M	MB	MB
	Robo de equipos	MA	MB	MB
	Acceso no autorizado	B	MB	MB
Servidor Earth (Portal Institucional)	Fuego	M	MB	MB
	Daños por agua	M	MB	MB
	Desastres naturales	M	MB	MB
	Desastres industriales	M	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB

	Equivocaciones por parte del administrador del sistema	M	MB	MB
	Errores de mantenimiento	M	MB	MB
	Robo de equipos	A	MB	MB
	Acceso no autorizado	B	MB	MB
Servidor Marte (Sistema de información misional SIM)	Fuego	MA	MB	MB
	Daños por agua	MA	MB	MB
	Desastres naturales	MA	MB	MB
	Desastres industriales	MA	MB	MB
	Caída del sistema por fallas de energía	MA	MB	MB
	Condiciones de temperatura no aptas	A	MB	MB
	Equivocaciones por parte del administrador del sistema	A	MB	MB
	Errores de mantenimiento	A	MB	MB
	Robo de equipos	MA	MB	A
	Acceso no autorizado	B	A	A
Servidor Jupiter (Software de gestión documental ORFEO)	Fuego	M	MB	MB
	Daños por agua	M	MB	MB
	Desastres naturales	M	MB	MB
	Desastres industriales	M	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB
	Equivocaciones por parte del administrador del sistema	B	MB	MB
	Errores de mantenimiento	M	MB	MB
	Robo de equipos	M	MB	MB
	Acceso no autorizado	B	MB	MB
Servidor Saturno (Control de inventarios)	Fuego	M	MB	MB
	Daños por agua	M	MB	MB
	Desastres naturales	M	MB	MB
	Desastres industriales	M	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB
	Errores de mantenimiento	M	MB	MB
	Robo de equipos	M	MB	MB
	Acceso no autorizado	B	MB	MB
Servidor Titan (Copias de respaldo Veeam Backup)	Fuego	M	MB	MB
	Daños por agua	M	MB	MB
	Desastres naturales	M	MB	MB
	Desastres industriales	M	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB

	Condiciones de temperatura no aptas	M	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB
	Errores de mantenimiento	M	MB	MB
	Robo de equipos	M	MB	MB
	Acceso no autorizado	B	MB	MB
Servidor Neptuno (Antivirus Bitdefender)	Fuego	M	MB	MB
	Daños por agua	M	MB	MB
	Desastres naturales	M	MB	MB
	Desastres industriales	M	MB	MB
	Caída del sistema por fallas de energía	B	MB	MB
	Condiciones de temperatura no aptas	B	MB	MB
	Equivocaciones por parte del administrador del sistema	B	MB	MB
	Errores de mantenimiento	M	MB	MB
	Robo de equipos	MB	MB	MB
	Acceso no autorizado	B	MB	MB
Servidor de virtualización	Fuego	M	MB	MB
	Daños por agua	M	MB	MB
	Desastres naturales	M	MB	MB
	Desastres industriales	M	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB
	Errores de mantenimiento	M	MB	MB
	Robo de equipos	A	MB	MB
	Acceso no autorizado	B	MB	MB
Equipos de cómputo	Fuego	M	MB	MB
	Daños por agua	M	MB	MB
	Desastres naturales	M	MB	MB
	Desastres industriales	M	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB
	Errores de mantenimiento	M	MB	MB
	Robo de equipos	M	MB	A
	Acceso no autorizado	B	MB	M

Fuente: Área de Tecnología ICPJ

Tabla 16. Impacto para la categoría: Infraestructura física

ACTIVO	AMENAZAS	DIMENSIONES		
		D	I	C
Lectores biométricos	Fuego	M	MB	MB
	Daños por agua	M	MB	MB
	Desastres naturales	M	MB	MB
	Desastres industriales	M	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB
	Condiciones de temperatura no aptas	B	MB	MB
	Equivocaciones por parte del administrador del sistema	B	MB	MB
	Errores de mantenimiento	M	MB	MB
	Robo de equipos	M	MB	MB
	Acceso no autorizado	B	MB	MB
Datacenter	Fuego	MA	MB	MB
	Daños por agua	MA	MB	MB
	Desastres naturales	MA	MB	MB
	Desastres industriales	MA	MB	MB
	Caída del sistema por fallas de energía	MA	MB	MB
	Condiciones de temperatura no aptas	A	MB	MB
	Equivocaciones por parte del administrador del sistema	A	MB	MB
	Errores de mantenimiento	A	MB	MB
	Robo de equipos	MA	MB	MB
	Acceso no autorizado	M	MB	MB
Switches	Fuego	MA	MB	MB
	Daños por agua	MA	MB	MB
	Desastres naturales	MA	MB	MB
	Desastres industriales	MA	MB	MB
	Caída del sistema por fallas de energía	MA	MB	MB
	Condiciones de temperatura no aptas	A	MB	MB
	Equivocaciones por parte del administrador del sistema	A	MB	MB
	Errores de mantenimiento	A	MB	MB
	Robo de equipos	MA	MB	MB
	Acceso no autorizado	M	MB	MB

Fuente: Área de Tecnología ICPJ

Evaluación del riesgo: En esta sub fase se mide el nivel de riesgo inherente de acuerdo a la formula
Riesgo inherente = Impacto x probabilidad

Tabla 17. Riesgo potencial en la categoría: Servicios

ACTIVO	AMENAZAS	IMPACTO			PROBABILIDAD	No. Riesgo	RIESGO		
		D	I	C			D	I	C
Controlador de dominio	Equivocaciones por parte del administrador del sistema	A	A	A	B	1	MA	MA	MA
	Modificación de la información	MB	MA	MA	B	2	MB	MA	MB
	Destrucción de la información	MA	MA	MA	MB	3	MB	MB	MB
	Fugas de información	M	MA	M	B	4	M	MA	M
	Caída del sistema por fallas de energía	A	MB	MB	MB	5	MB	MB	MB
	Suplantación de la identidad del usuario	MB	A	A	B	6	MB	MA	MB
	Abuso de privilegios de acceso	MB	A	A	M	7	MB	MA	MB
	Acceso no autorizado	MB	A	A	B	8	MB	MA	MB
Controlador de dominio alterno	Equivocaciones por parte del administrador del sistema	A	A	A	B	9	MA	MA	MA
	Modificación de la información	MB	MA	MA	B	10	MB	MA	MB
	Destrucción de la información	MA	MA	MA	MB	11	MB	MB	MB
	Fugas de información	M	MA	M	B	12	M	MA	M
	Caída del sistema por fallas de energía	A	MB	MB	B	13	MA	MB	MA
	Suplantación de la identidad del usuario	MB	A	A	B	14	MB	MA	MB
	Abuso de privilegios de acceso	MB	A	A	B	15	MB	MA	MB
	Acceso no autorizado	MB	A	A	B	16	MB	MA	MB
Correo electrónico G-SUITE	Equivocaciones por parte del administrador del sistema	MB	MB	MB	MB	17	MB	MB	MB
	Modificación de la información	MB	MB	MB	MB	18	MB	MB	MB
	Destrucción de la información	B	B	MB	B	19	B	B	B
	Fugas de información	MB	MB	B	B	20	MB	MB	MB
	Caída del sistema por fallas de energía	MB	MB	MB	MB	21	MB	MB	MB
	Suplantación de la identidad del usuario	MB	MB	MB	MB	22	MB	MB	MB
	Abuso de privilegios de acceso	MB	B	B	MB	23	MB	MB	MB
	Acceso no autorizado	MB	MB	MB	B	24	MB	MB	MB
	Errores por parte de los usuarios	MB	B	B	B	25	MB	B	MB
Portal Institucional	Equivocaciones por parte del administrador del sistema	A	A	MB	MB	26	MB	MB	MB
	Modificación de la información	MB	A	MB	B	27	MB	MA	MB
	Destrucción de la información	MB	A	MB	B	28	MB	MA	MB
	Fugas de información	MB	A	MB	MB	29	MB	MB	MB
	Caída del sistema por fallas de energía	MA	MA	MB	MB	30	MB	MB	MB
	Suplantación de la identidad del usuario	A	A	MB	MB	31	MB	MB	MB
	Abuso de privilegios de acceso	M	M	MB	M	32	MA	MA	MA

	Acceso no autorizado	A	A	MB	B	33	MA	MA	MA
	Errores por parte de los usuarios	MB	MB	MB	B	34	MB	MB	MB
	Errores de monitorización (log)	B	B	MB	B	35	B	B	B
	Errores de configuración	A	A	MB	B	36	MA	MA	MA
	Vulnerabilidades en la página web	A	A	MB	M	37	MA	MA	MA
	Errores de mantenimiento	M	M	MB	M	38	MA	MA	MA
	Caída del sistema por fallas de energía	MB	MB	MB	MB	39	MB	MB	MB
	Intrusión de código malicioso	M	M	MB	B	40	M	M	M
	Denegación de servicio	B	MB	MB	B	41	B	MB	B
Canal de internet y red MPLS	Fuego	MA	MB	MB	B	42	MA	MB	MA
	Daños por agua	MA	MB	MB	MB	43	MB	MB	MB
	Desastres naturales	MA	MB	MB	B	44	MA	MB	MA
	Avería de origen físico o lógico	MA	MB	MB	B	45	MA	MB	MA
	Caída del sistema por fallas de energía	A	MB	MB	B	46	MA	MB	MA
	Condiciones inadecuadas de temperatura o humedad	A	MB	MB	B	47	MA	MB	MA
	Interrupción deliberada por un agente externo	A	MB	MB	B	48	MA	MB	MA
	Errores de configuración	A	MB	MB	MB	49	MB	MB	MB
	Errores de mantenimiento / actualización de equipos (hardware)	A	MB	MB	B	50	MA	MB	MA
	Robo de equipos	MA	MB	MB	B	51	MA	MB	MA
Acceso a red privada virtual (VPN)	Equivocaciones por parte del administrador del sistema	A	MB	MB	B	52	MA	MB	MA
	Fugas de información	M	MB	MB	B	53	M	MB	M
	Suplantación de la identidad del usuario	M	MB	MB	M	54	MA	MB	MA
	Abuso de privilegios de acceso	A	MB	MB	MB	55	MB	MB	MB
	Acceso no autorizado	A	MB	MB	B	56	MA	MB	MA
	Errores por parte de los usuarios	MB	MB	MB	B	57	MB	MB	MB

Fuente: Área de Tecnología ICPJ

Tabla 18. Riesgo potencial en la categoría: Aplicaciones

ACTIVO	AMENAZAS	IMPACTO			PROBABILIDAD	No. Riesgo	RIESGO		
		D	I	C			D	I	C
Sistema de información misional SIM	Errores por parte de los usuarios	MB	MB	MB	B	58	MB	MB	MB
	Equivocaciones por parte del administrador del sistema	MA	MA	MA	B	59	MA	MA	MA
	Errores de monitorización (log)	MB	MB	MB	B	60	MB	MB	MB
	Errores de configuración	MA	MA	MA	B	61	MA	MA	MA
	Modificación de la información	MB	MA	MA	B	62	MB	MA	MA
	Errores de mantenimiento	A	A	MB	M	63	MA	MA	MB
	Caída del sistema por fallas de energía	MA	MB	MB	B	64	MA	MB	MB
	Intrusión de código malicioso	MA	MA	MA	M	65	MA	MA	MA
	Denegación de servicio	MA	MB	MB	M	66	MA	MB	MB
Software de Sistemas operativos	Errores por parte de los usuarios	B	MB	MB	B	67	B	MB	MB
	Equivocaciones por parte del administrador del sistema	A	A	MB	MB	68	MB	MB	MB
	Errores de monitorización (log)	MB	MB	MB	B	69	MB	MB	MB
	Errores de configuración	M	MB	MB	B	70	M	MB	MB
	Modificación de la información	B	MB	MB	B	71	B	MB	MB
	Errores de mantenimiento	MA	MA	MB	B	72	MA	MA	MB
	Caída del sistema por fallas de energía	MA	MB	MB	B	73	MA	MB	MB
	Intrusión de código malicioso	MA	MA	MA	M	74	MA	MA	MA
Software de Base de Datos	Equivocaciones por parte del administrador del sistema	MA	M	MB	B	75	MA	M	MB
	Errores de monitorización (log)	MB	MB	MB	B	76	MB	MB	MB
	Errores de configuración	M	M	MB	B	77	M	M	MB
	Modificación de la información	B	MA	MB	B	78	B	MA	MB
	Errores de mantenimiento	A	B	MB	B	79	A	B	MB
	Caída del sistema por fallas de energía	A	B	MB	B	80	A	B	MB
	Intrusión de código malicioso	MA	MA	MA	B	81	MA	MA	MA
Software de Aplicaciones Ofimáticas	Errores por parte de los usuarios	B	MB	MB	B	82	B	MB	MB
	Errores de configuración	B	MB	MB	B	83	B	MB	MB
	Modificación de la información	A	B	B	B	84	A	B	B
	Errores de mantenimiento	M	B	B	B	85	M	B	B
	Intrusión de código malicioso	A	A	MB	B	86	A	A	MB
Software de gestión documental ORFEO	Errores por parte de los usuarios	B	B	A	B	87	B	B	A
	Equivocaciones por parte del administrador del sistema	MA	MA	MA	B	88	MA	MA	MA
	Errores de monitorización (log)	MB	MB	MB	B	89	MB	MB	MB
	Errores de configuración	A	A	A	B	90	A	A	A
	Modificación de la información	B	MA	M	B	91	B	MA	M
	Errores de mantenimiento	A	A	A	M	92	MA	MA	MA
	Caída del sistema por fallas de energía	MA	MB	MB	B	93	MA	MB	MB
	Intrusión de código malicioso	MA	MA	MA	MB	94	MB	MB	MB

Software para el control de inventarios	Errores por parte de los usuarios	MB	B	B	B	95	MB	B	B
	Equivocaciones por parte del administrador del sistema	A	A	A	B	96	A	A	A
	Errores de monitorización (log)	MB	MB	MB	B	97	MB	MB	MB
	Errores de configuración	A	A	A	B	98	A	A	A
	Modificación de la información	MB	MA	B	B	99	MB	MA	B
	Errores de mantenimiento	A	M	MB	B	100	A	M	MB
	Caída del sistema por fallas de energía	MA	B	MB	B	101	MA	B	MB
	Intrusión de código malicioso	MA	MA	MA	M	102	MA	MA	MA
	Denegación de servicio	MA	B	MB	M	103	MA	M	MB
Software para copias de respaldo Veeam Backup	Equivocaciones por parte del administrador del sistema	MA	A	M	B	104	MA	A	M
	Errores de monitorización (log)	MB	MB	MB	B	105	MB	MB	MB
	Errores de configuración	A	A	MB	B	106	A	A	MB
	Modificación de la información	MB	MA	MB	B	107	MB	MA	MB
	Errores de mantenimiento	A	A	MB	M	108	MA	MA	MB
	Caída del sistema por fallas de energía	MA	M	MB	B	109	MA	M	MB
	Intrusión de código malicioso	MA	MA	MA	B	110	MA	MA	MA
Software de virtualización	Equivocaciones por parte del administrador del sistema	MA	A	M	B	111	MA	A	M
	Errores de monitorización (log)	MB	MB	MB	B	112	MB	MB	MB
	Errores de configuración	A	A	MB	B	113	A	A	MB
	Modificación de la información	MB	MA	MB	B	114	MB	MA	MB
	Errores de mantenimiento	A	A	MB	M	115	MA	MA	MB
	Caída del sistema por fallas de energía	MA	M	MB	B	116	MA	M	MB
	Intrusión de código malicioso	MA	MA	MA	B	117	MA	MA	MA
Software de acceso biométrico	Errores por parte de los usuarios	MB	MB	MB	MB	118	MB	MB	MB
	Equivocaciones por parte del administrador del sistema	A	A	MB	MB	119	MB	MB	MB
	Errores de monitorización (log)	MB	MB	MB	B	120	MB	MB	MB
	Errores de configuración	A	A	MB	B	121	A	A	MB
	Modificación de la información	MB	MA	MB	B	122	MB	MA	MB
	Errores de mantenimiento	A	MB	MB	MB	123	MB	MB	MB
	Caída del sistema por fallas de energía	M	B	MB	M	124	MA	M	MB
	Intrusión de código malicioso	MA	MA	MA	MB	125	MB	MB	MB
	Denegación de servicio	MA	B	MB	MB	126	MB	MB	MB
Antivirus Bitdefender	Errores por parte de los usuarios	B	B	B	B	127	B	B	B
	Equivocaciones por parte del administrador del sistema	M	B	MB	MB	128	MB	MB	MB
	Errores de monitorización (log)	MB	MB	MB	B	129	MB	MB	MB
	Errores de configuración	M	B	MB	B	130	M	B	MB
	Modificación de la información	M	B	MB	B	131	M	B	MB
	Caída del sistema por fallas de energía	B	B	MB	MB	132	MB	MB	MB
	Errores de mantenimiento	B	B	MB	B	133	B	B	MB
	Abuso de privilegios de acceso	B	B	MB	B	134	B	B	MB

Fuente: Área de Tecnología ICPJ

Tabla 19. Riesgo potencial en la categoría: Información

ACTIVO	AMENAZAS	IMPACTO			PROBABILIDAD	No. Riesgo	RIESGO		
		D	I	C			D	I	C
Información digital	Errores de configuración	B	B	B	B	135	B	B	B
	Errores de monitorización (log)	MB	MB	MB	B	136	MB	MB	MB
	Alteración de la información	MB	MA	MB	B	137	MB	MA	MB
	Errores de mantenimiento	A	M	MB	B	138	A	M	MB
	Intrusión de código malicioso	M	M	A	B	139	MA	MA	MA

Fuente: Área de Tecnología ICPJ

Tabla 20. Riesgo potencial en la categoría: Equipos

ACTIVO	AMENAZAS	IMPACTO			PROBABILIDAD	No. Riesgo	RIESGO		
		D	I	C			D	I	C
Firewall Palo Alto	Fuego	M	MB	MB	B	140	M	MB	MB
	Daños por agua	M	MB	MB	M	141	MA	MB	MB
	Desastres naturales	M	MB	MB	B	142	M	MB	MB
	Desastres industriales	M	MB	MB	MB	143	MB	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB	B	144	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB	M	145	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB	B	146	M	MB	MB
	Errores de mantenimiento	MA	MB	MB	M	147	MA	MB	MB
	Robo de equipos	MA	MB	MB	MB	148	MB	MB	MB
	Acceso no autorizado	B	MB	MB	B	149	B	MB	MB
Servidor Mercurio (Active Directory Principal)	Fuego	A	MB	MB	B	150	A	MB	MB
	Daños por agua	A	MB	MB	M	151	MA	MB	MB
	Desastres naturales	A	MB	MB	B	152	A	MB	MB
	Desastres industriales	A	MB	MB	MB	153	MB	MB	MB
	Caída del sistema por fallas de energía	A	MB	MB	B	154	A	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB	M	155	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB	B	156	M	MB	MB
	Errores de mantenimiento	M	MB	MB	M	157	MA	MB	MB
	Robo de equipos	MA	MB	MB	MB	158	MB	MB	MB
	Acceso no autorizado	B	MB	MB	B	159	B	MB	MB
Servidor Venus (Active Directory Secundario)	Fuego	A	MB	MB	B	160	A	MB	MB
	Daños por agua	A	MB	MB	B	161	A	MB	MB
	Desastres naturales	A	MB	MB	B	162	A	MB	MB
	Desastres industriales	A	MB	MB	MB	163	MB	MB	MB
	Caída del sistema por fallas de energía	A	MB	MB	B	164	A	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB	M	165	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB	B	166	M	MB	MB
	Errores de mantenimiento	M	MB	MB	M	167	MA	MB	MB
	Robo de equipos	MA	MB	MB	MB	168	MB	MB	MB
	Acceso no autorizado	B	MB	MB	B	169	B	MB	MB
Servidor Earth (Portal Institucional)	Fuego	M	MB	MB	B	170	M	MB	MB
	Daños por agua	M	MB	MB	M	171	MA	MB	MB
	Desastres naturales	M	MB	MB	B	172	M	MB	MB
	Desastres industriales	M	MB	MB	MB	173	MB	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB	B	174	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB	M	175	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB	B	176	M	MB	MB

	Errores de mantenimiento	M	MB	MB	M	177	MA	MB	MB
	Robo de equipos	A	MB	MB	MB	178	MB	MB	MB
	Acceso no autorizado	B	MB	MB	B	179	B	MB	MB
Servidor Marte (Sistema de información misional SIM)	Fuego	MA	MB	MB	B	180	MA	MB	MB
	Daños por agua	MA	MB	MB	M	181	MA	MB	MB
	Desastres naturales	MA	MB	MB	B	182	MA	MB	MB
	Desastres industriales	MA	MB	MB	MB	183	MB	MB	MB
	Caída del sistema por fallas de energía	MA	MB	MB	B	184	MA	MB	MB
	Condiciones de temperatura no aptas	A	MB	MB	M	185	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	A	MB	MB	B	186	A	MB	MB
	Errores de mantenimiento	A	MB	MB	M	187	MA	MB	MB
	Robo de equipos	MA	MB	A	MB	188	MB	MB	MB
	Acceso no autorizado	B	A	A	B	189	B	A	A
Servidor Jupiter (Software de gestión documental ORFEO)	Fuego	M	MB	MB	B	190	M	MB	MB
	Daños por agua	M	MB	MB	M	191	MA	MB	MB
	Desastres naturales	M	MB	MB	B	192	M	MB	MB
	Desastres industriales	M	MB	MB	MB	193	MB	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB	B	194	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB	M	195	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	B	MB	MB	B	196	B	MB	MB
	Errores de mantenimiento	M	MB	MB	M	197	MA	MB	MB
	Robo de equipos	M	MB	MB	MB	198	MB	MB	MB
	Acceso no autorizado	B	MB	MB	B	199	B	MB	MB
Servidor Saturno (Control de inventarios)	Fuego	M	MB	MB	B	200	M	MB	MB
	Daños por agua	M	MB	MB	M	201	MA	MB	MB
	Desastres naturales	M	MB	MB	B	202	M	MB	MB
	Desastres industriales	M	MB	MB	MB	203	MB	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB	B	204	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB	M	205	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB	B	206	M	MB	MB
	Errores de mantenimiento	M	MB	MB	M	207	MA	MB	MB
	Robo de equipos	M	MB	MB	MB	208	MB	MB	MB
	Acceso no autorizado	B	MB	MB	B	209	B	MB	MB
Servidor Titan (Copias de respaldo Veeam Backup)	Fuego	M	MB	MB	B	210	M	MB	MB
	Daños por agua	M	MB	MB	M	211	MA	MB	MB
	Desastres naturales	M	MB	MB	B	212	M	MB	MB
	Desastres industriales	M	MB	MB	MB	213	MB	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB	B	214	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB	M	215	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB	B	216	M	MB	MB
	Errores de mantenimiento	M	MB	MB	M	217	MA	MB	MB

	Robo de equipos	M	MB	MB	MB	218	MB	MB	MB
	Acceso no autorizado	B	MB	MB	B	219	B	MB	MB
Servidor Neptuno (Antivirus Bitdefender)	Fuego	M	MB	MB	B	220	M	MB	MB
	Daños por agua	M	MB	MB	M	221	MA	MB	MB
	Desastres naturales	M	MB	MB	B	222	M	MB	MB
	Desastres industriales	M	MB	MB	MB	223	MB	MB	MB
	Caída del sistema por fallas de energía	B	MB	MB	B	224	B	MB	MB
	Condiciones de temperatura no aptas	B	MB	MB	M	225	M	MB	MB
	Equivocaciones por parte del administrador del sistema	B	MB	MB	B	226	B	MB	MB
	Errores de mantenimiento	M	MB	MB	M	227	MA	MB	MB
	Robo de equipos	MB	MB	MB	MB	228	MB	MB	MB
	Acceso no autorizado	B	MB	MB	B	229	B	MB	MB
Servidor de virtualización	Fuego	M	MB	MB	B	230	M	MB	MB
	Daños por agua	M	MB	MB	M	231	MA	MB	MB
	Desastres naturales	M	MB	MB	B	232	M	MB	MB
	Desastres industriales	M	MB	MB	MB	233	MB	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB	B	234	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB	M	235	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB	B	236	M	MB	MB
	Errores de mantenimiento	M	MB	MB	M	237	MA	MB	MB
	Robo de equipos	A	MB	MB	MB	238	MB	MB	MB
	Acceso no autorizado	B	MB	MB	B	239	B	MB	MB
Equipos de cómputo	Fuego	M	MB	MB	B	240	M	MB	MB
	Daños por agua	M	MB	MB	M	241	MA	MB	MB
	Desastres naturales	M	MB	MB	B	242	M	MB	MB
	Desastres industriales	M	MB	MB	MB	243	MB	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB	B	244	M	MB	MB
	Condiciones de temperatura no aptas	M	MB	MB	M	245	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	M	MB	MB	B	246	M	MB	MB
	Errores de mantenimiento	M	MB	MB	M	247	MA	MB	MB
	Robo de equipos	M	MB	A	M	248	MA	MB	MA
	Acceso no autorizado	B	MB	M	B	249	B	MB	M

Fuente: Área de Tecnología ICPJ

Tabla 21. Riesgo potencial en la categoría: Infraestructura física

ACTIVO	AMENAZAS	IMPACTO			PROBABILIDAD	No. Riesgo	RIESGO		
		D	I	C			D	I	C
Lectores biométricos	Fuego	M	MB	MB	B	250	M	MB	MB
	Daños por agua	M	MB	MB	M	251	MA	MB	MB
	Desastres naturales	M	MB	MB	B	252	M	MB	MB
	Desastres industriales	M	MB	MB	MB	253	MB	MB	MB
	Caída del sistema por fallas de energía	M	MB	MB	M	254	MA	MB	MB
	Condiciones de temperatura no aptas	B	MB	MB	B	255	B	MB	MB
	Equivocaciones por parte del administrador del sistema	B	MB	MB	B	256	B	MB	MB
	Errores de mantenimiento	M	MB	MB	M	257	MA	MB	MB
	Robo de equipos	M	MB	MB	MB	258	MB	MB	MB
	Acceso no autorizado	B	MB	MB	MB	259	MB	MB	MB
DataCenter	Fuego	MA	MB	MB	B	260	MA	MB	MB
	Daños por agua	MA	MB	MB	M	261	MA	MB	MB
	Desastres naturales	MA	MB	MB	B	262	MA	MB	MB
	Desastres industriales	MA	MB	MB	MB	263	MB	MB	MB
	Caída del sistema por fallas de energía	MA	MB	MB	B	264	MA	MB	MB
	Condiciones de temperatura no aptas	A	MB	MB	M	265	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	A	MB	MB	B	266	A	MB	MB
	Errores de mantenimiento	A	MB	MB	B	267	A	MB	MB
	Robo de equipos	MA	MB	MB	MB	268	MB	MB	MB
	Acceso no autorizado	M	MB	MB	B	269	M	MB	MB
Switches	Fuego	MA	MB	MB	B	270	MA	MB	MB
	Daños por agua	MA	MB	MB	M	271	MA	MB	MB
	Desastres naturales	MA	MB	MB	B	272	MA	MB	MB
	Desastres industriales	MA	MB	MB	MB	273	MB	MB	MB
	Caída del sistema por fallas de energía	MA	MB	MB	M	274	MA	MB	MB
	Condiciones de temperatura no aptas	A	MB	MB	M	275	MA	MB	MB
	Equivocaciones por parte del administrador del sistema	A	MB	MB	B	276	A	MB	MB
	Errores de mantenimiento	A	MB	MB	M	277	MA	MB	MB
	Robo de equipos	MA	MB	MB	M	278	MA	MB	MB
	Acceso no autorizado	M	MB	MB	B	279	M	MB	MB

Fuente: Área de Tecnología ICPJ

Mapa de calor

Teniendo en cuenta el siguiente criterio de evaluación se realizó el mapa de calor.

Tabla 22. Criterios de Riesgo

Riesgo	
5	Muy alto
4	Alto
3	Medio
2	Bajo
1	Muy bajo

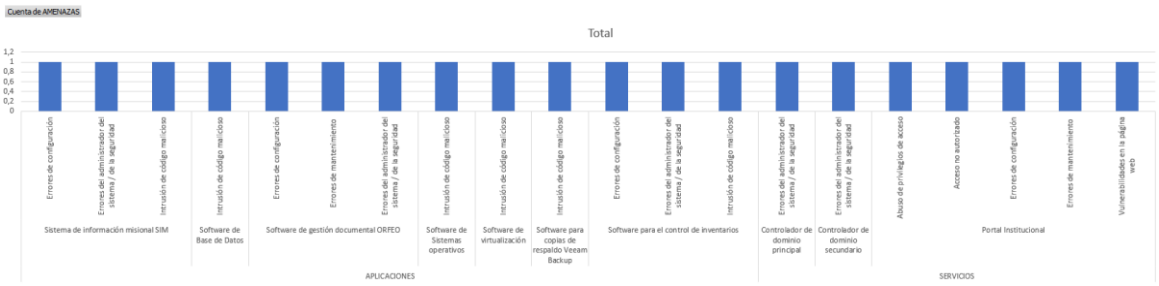
Tabla 23. Activos con riesgos más altos a bajos

TIPO	ACTIVO	AMENAZAS	Valor Riesgo
Servicios	**Controlador de dominio**	Equivocaciones por parte del administrador del sistema	5
Servicios	**Controlador de dominio**	Destrucción de la información	1
Servicios	**Controlador de dominio**	Caída del sistema por fallas de energía	1
Servicios	**Controlador de dominio alterno**	Equivocaciones por parte del administrador del sistema	5
Servicios	**Controlador de dominio alterno**	Destrucción de la información	1
Servicios	**Correo electrónico G-SUITE**	Equivocaciones por parte del administrador del sistema	1
Servicios	**Correo electrónico G-SUITE**	Modificación de la información	1
Servicios	**Correo electrónico G-SUITE**	Destrucción de la información	2
Servicios	**Correo electrónico G-SUITE**	Fugas de información	1
Servicios	**Correo electrónico G-SUITE**	Caída del sistema por fallas de energía	1
Servicios	**Correo electrónico G-SUITE**	Suplantación de la identidad del usuario	1
Servicios	**Correo electrónico G-SUITE**	Abuso de privilegios de acceso	1
Servicios	**Correo electrónico G-SUITE**	Acceso no autorizado	1
Servicios	**Portal Institucional**	Equivocaciones por parte del administrador del sistema	1
Servicios	**Portal Institucional**	Fugas de información	1
Servicios	**Portal Institucional**	Caída del sistema por fallas de energía	1

Servicios	**Portal Institucional**	Suplantación de la identidad del usuario	1
Servicios	**Portal Institucional**	Abuso de privilegios de acceso	5
Servicios	**Portal Institucional**	Acceso no autorizado	5
Servicios	**Portal Institucional**	Errores por parte de los usuarios	1
Servicios	**Portal Institucional**	Errores de monitorización (log)	2
Servicios	**Portal Institucional**	Errores de configuración	5
Servicios	**Portal Institucional**	Vulnerabilidades en la página web	5
Servicios	**Portal Institucional**	Errores de mantenimiento	5
Servicios	**Portal Institucional**	Caída del sistema por fallas de energía	1
Servicios	**Portal Institucional**	Intrusión de código malicioso	3
Servicios	**Canal de internet y red MPLS**	Daños por agua	1
Servicios	**Canal de internet y red MPLS**	Errores de configuración	1
Servicios	**Acceso a red privada virtual (VPN)**	Abuso de privilegios de acceso	1
Servicios	**Acceso a red privada virtual (VPN)**	Errores por parte de los usuarios	1
Aplicaciones	**Sistema de información misional SIM**	Errores por parte de los usuarios	1
Aplicaciones	**Sistema de información misional SIM**	Equivocaciones por parte del administrador del sistema	5
Aplicaciones	**Sistema de información misional SIM**	Errores de monitorización (log)	1
Aplicaciones	**Sistema de información misional SIM**	Errores de configuración	5
Aplicaciones	**Sistema de información misional SIM**	Intrusión de código malicioso	5
Aplicaciones	**Software de Sistemas operativos**	Equivocaciones por parte del administrador del sistema	1
Aplicaciones	**Software de Sistemas operativos**	Errores de monitorización (log)	1
Aplicaciones	**Software de Sistemas operativos**	Intrusión de código malicioso	5
Aplicaciones	**Software de Base de Datos**	Errores de monitorización (log)	1
Aplicaciones	**Software de Base de Datos**	Intrusión de código malicioso	5
Aplicaciones	**Software de gestión documental ORFEO**	Equivocaciones por parte del administrador del sistema	5
Aplicaciones	**Software de gestión documental ORFEO**	Errores de monitorización (log)	1
Aplicaciones	**Software de gestión documental ORFEO**	Errores de configuración	4
Aplicaciones	**Software de gestión documental ORFEO**	Errores de mantenimiento	5

Aplicaciones	**Software de gestión documental ORFEO**	Intrusión de código malicioso	1
Aplicaciones	**Software para el control de inventarios**	Equivocaciones por parte del administrador del sistema	4
Aplicaciones	**Software para el control de inventarios**	Errores de monitorización (log)	1
Aplicaciones	**Software para el control de inventarios**	Errores de configuración	4
Aplicaciones	**Software para el control de inventarios**	Intrusión de código malicioso	5
Aplicaciones	**Software para copias de respaldo Veeam Backup**	Errores de monitorización (log)	1
Aplicaciones	**Software para copias de respaldo Veeam Backup**	Intrusión de código malicioso	5
Aplicaciones	**Software de virtualización**	Errores de monitorización (log)	1
Aplicaciones	**Software de virtualización**	Intrusión de código malicioso	5
Aplicaciones	**Software de acceso biométrico**	Errores por parte de los usuarios	1
Aplicaciones	**Software de acceso biométrico**	Equivocaciones por parte del administrador del sistema	1
Aplicaciones	**Software de acceso biométrico**	Errores de monitorización (log)	1
Aplicaciones	**Software de acceso biométrico**	Errores de mantenimiento	1
Aplicaciones	**Software de acceso biométrico**	Intrusión de código malicioso	1
Aplicaciones	**Software de acceso biométrico**	Denegación de servicio	1
Aplicaciones	**Antivirus Bitdefender**	Errores por parte de los usuarios	2
Aplicaciones	**Antivirus Bitdefender**	Equivocaciones por parte del administrador del sistema	1
Aplicaciones	**Antivirus Bitdefender**	Errores de monitorización (log)	1
Aplicaciones	**Antivirus Bitdefender**	Caída del sistema por fallas de energía	1
Información	**Información digital**	Errores de configuración	2
Información	**Información digital**	Errores de monitorización (log)	1
Equipos	**Firewall Palo 4**	Desastres industriales	1
Equipos	**Firewall Palo 4**	Robo de equipos	1
Equipos	**Servidor Mercurio (Active Directory Principal)**	Desastres industriales	1
Equipos	**Servidor Mercurio (Active Directory Principal)**	Robo de equipos	1
Equipos	**Servidor Venus (Active Directory Secundario)**	Desastres industriales	1
Equipos	**Servidor Venus (Active Directory Secundario)**	Robo de equipos	1

Equipos	**Servidor Earth (Portal Institucional)**	Desastres industriales	1
Equipos	**Servidor Earth (Portal Institucional)**	Robo de equipos	1
Equipos	**Servidor Marte (Sistema de información misional SIM)**	Desastres industriales	1
Equipos	**Servidor Marte (Sistema de información misional SIM)**	Robo de equipos	1
Equipos	**Servidor Jupiter (Software de gestión documental ORFEO)**	Desastres industriales	1
Equipos	**Servidor Jupiter (Software de gestión documental ORFEO)**	Robo de equipos	1
Equipos	**Servidor Saturno (Control de inventarios)**	Desastres industriales	1
Equipos	**Servidor Saturno (Control de inventarios)**	Robo de equipos	1
Equipos	**Servidor Titan (Copias de respaldo Veeam Backup)**	Desastres industriales	1
Equipos	**Servidor Titan (Copias de respaldo Veeam Backup)**	Robo de equipos	1
Equipos	**Servidor Neptuno (Antivirus Bitdefender)**	Desastres industriales	1
Equipos	**Servidor Neptuno (Antivirus Bitdefender)**	Robo de equipos	1
Equipos	**Servidor de virtualización**	Desastres industriales	1
Equipos	**Servidor de virtualización**	Robo de equipos	1
Equipos	**Equipos de cómputo**	Desastres industriales	1
Infraestructura	**Lectores biométricos**	Desastres industriales	1
Infraestructura	**Lectores biométricos**	Robo de equipos	1
Infraestructura	**Lectores biométricos**	Acceso no autorizado	1
Infraestructura	**Datacenter**	Desastres industriales	1
Infraestructura	**Datacenter**	Robo de equipos	1
Infraestructura	**Switches**	Desastres industriales	1



Fuente: Área de Tecnología ICPJ

Realizada la evaluación de los activos y conociendo los riesgos a los que se encuentran expuestos los mismos, se escogen los activos que tengan una valoración alta o superior en sus tres pilares de la seguridad de la información.

Los activos cuyos riesgos son se encuentran catalogados como altos o muy altos: el Controlador de dominio y secundario, el portal institucional, el sistema de información misional SIM, los sistemas operativos, el software de base de datos, software de gestión documental ORFEO, software para el control de inventarios, software para copias de respaldo y de virtualización.

Declaración de Aplicabilidad

A continuación, se muestra los controles pertenecientes a la norma ISO 27001 los cuales se encuentran en el anexo A[117] y se relacionan con el ICPJ con el fin de determinar si los controles mencionados son obligatorios en la entidad y cuáles son las observaciones frente a su estado actual en el ICPJ:

Tabla 24. Declaración de aplicabilidad

Control principal	Código del control	Objetivos del control	Descripción del control	¿Es un requerimiento obligatorio en el ICPJ?	Observaciones del estado actual del control en el ICPJ
Políticas de la seguridad de la información	A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de lainformación, aprobada por la dirección, publicada y comunicada a losempleados y a las partes externas pertinentes.	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información se deben revisar aintervalos planificados, o si ocurren cambios significativos, para asegurarsu conveniencia, adecuación y eficacia continúas.	SI	El control esta implementado y se puede encontrar en el numeral 5 del manual de politica de seguridad para el manejo de la información
Organización de la seguridad de la información	A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.6.1.3	Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.6.1.4	Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	NO	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	NO	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.6.2.1	Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles	NO	El control no esta implementado de manera correcta ya que el ICPJ a pesar de contar con redes wifi para conexión de dispositivos moviles no cuenta con ningun tipo de evidencia de las conexiones realizadas, los dispositivos que conectaron a dichas redes wifi, eventos de estas conexiones, etc.
	A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo	NO	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.

[117] Norma Técnica Colombiana NTC-ISO/IEC 27001, Anexo A, p.21

Seguridad de los recursos humanos	A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	NO	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	NO	El control esta implementado, el área de TI realiza la divulgación acerca de la aplicación de la seguridad de la información a todos los funcionarios de la entidad.
	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	SI	El control esta implementado, este se lleva a traves de capacitaciones por parte del área de TI a los funcionarios de la entidad sobre la importancia de la seguridad de la información, como evidencia se encuentran las actas.
	A.7.2.3	Proceso disciplinario	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI	El control esta implementado, las acciones son realizadas por el área de control interno disciplinario quienes a tráves de memorandos y actas llevan su respectiva evidencia.
	A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	SI	El control esta implementado, es ejecutado por el área de desarrollo humano, realiza y envia memorandos a las áreas donde un funcionario termina su contrato con el fin de que dicha área emita un paz y salvo constatando de que el funcionario uso y entrego la información asignada de manera adecuada.
Gestión de activos	A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	SI	El control esta implementado, y se puede encontrar a tráves del proceso Gestión Tecnológica de la información.
	A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario	SI	El control esta implementado, y se puede encontrar a tráves del proceso control de inventarios.
	A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	SI	El control esta implementado, a tráves del formato seguimiento de bienes de consumo controlado y/o devolutivos dentro de una misma dependencia, una vez un funcionario termine su vinculacion con la entidad este debera devolver los bienes asignado a su cargo para poder darle su paz y salvo y de esta manera lograr su desvinculación de manera éxitosa.
	A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.8.3.2	Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	SI	El control esta implementado, el área de TI realiza copias de la información de la entidad en cintas para posteriormente darlas en custodia a un tercero.

Control de acceso	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.9.1.2	Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente	NO	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	SI	El control esta implementado de manera parcial, se crean y asignan los usuarios en el directorio activo el cual esta sincronizado con los diferentes sistemas de información, pero no existe ningun procedimiento formal de registro debidamente documentado acerca de la creacion o cancelacion de los usuarios.
	A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.9.2.4	Gestión de información de autenticación secreta	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	NO	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.9.4.5	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas	NO	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
Criptografía	A.10.1.1	Política sobre el uso de controles	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	NO	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.

Seguridad física y del entorno	A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	SI	El control esta implementado, se encuentra definido en la politica de seguridad fisica de los activos tangibles de la entidad y esta debe hacerla cumplir la empresa que presta el servicio de vigilancia.
	A.11.1.2	11.1.2 Controles de acceso físicos	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.	SI	El control esta implementado, se encuentra definido en la politica de seguridad fisica de los activos tangibles de la entidad y esta debe hacerla cumplir la empresa que presta el servicio de vigilancia.
	A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones	SI	El control esta implementado, pero se debe documentar a un mayor detalle puesot que se encuentra a un nivel muy general.
	A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	El control esta implementado, pero se debe reforzar, puesto que en varias sedes de la entidad no cuentan con dispositivos clave como sensores de humo y gas.
	A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.11.1.6	Áreas de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	SI	El control esta implementado y se encuentra politica de seguridad y proteccion de equipos de TI.
	A.11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI	El control esta implementado pero debe reforzarse ya que hay varias unidades de la entidad que no estan protegidas contra fallas de energia.
	A.11.2.3	Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño	SI	El control esta implementado pero se debe revisar y actualizar la documentacion.
	A.11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas	SI	El control esta implementado, este se lleva a tráves del formato de mantenimiento preventivo y correctivo de los equipos de computo.
	A.11.2.5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	SI	El control esta implementado y se ejecuta según la politica de manejo de activos.
	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.11.2.7	Disposición segura o reutilización de equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reuso.	SI	El control esta implementado pero debe reforzarse puesto que en diferentes ocasiones no se deja evidencia de ello.
	A.11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	SI	El control esta implementado y se puede encontrar en la politica de gestión ambiental de la entidad.

Seguridad de las operaciones	A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	SI	El control esta implementado pero se debe reforzar ya que en varias áreas de la entidad se encuentra incompleto.
	A.12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.12.1.3	Gestión de capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	SI	El control esta implementado pero no existe ninguna documentación de los procedimientos que se llevan a cabo.
	A.12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI	El control esta implementado y se encuentra documentado a tráves de la politica de seguridad perimetral.
	A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	SI	El control esta implementado y se registra la evidencia a tráves del formato de backups de información.
	A.12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	SI	El control esta implementado y se realiza a tráves del protocolo PTP.
	A.12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.12.6.2	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.12.7	Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.

Seguridad de las comunicaciones	A.13.1.1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI	El control esta implementado a través del firewall pero no existe documentación sobre el procedimiento que se lleva.
	A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	SI	El control esta implementado a través del firewall y switches pero no existe documentación sobre el procedimiento que se lleva.
	A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SI	El control esta implementado a través del firewall y switches pero no existe documentación sobre el procedimiento que se lleva.
	A.13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	NO	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	NO	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SI	El control esta implementado a tráves de la plataforma de G-Suite y los procedimientos establecidos se encuentran en la politica de seguridad para el manejo de la información
	A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.

Seguridad en los procesos de desarrollo y de soporte	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	SI	El control esta implementado pero debe documentarse mejor.
	A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	SI	El control esta implementado a traves del firewall pero se deben documentar mejor los procedimientos.
	A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	SI	El control esta implementado a tráves del codigo creado y puesto en marcha para esta labor, pero no se evidencia ningun tipo de documentacion donde se encuentre la proteccion de transacciones.
	A.14.2.1	Política de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.14.2.2	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	SI	El control esta implementado y se documentan en los formatos de TI desarrollo y /o actualizacion de software.
	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.14.2.4	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.14.2.5	Principios de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	SI	El control esta implementado pero la documentacion se encuentra incompleta.
	A.14.2.7	Desarrollo contratado	La organización debe supervisar y hacer	SI	El control esta implementado pero se debe reforzar ya
	A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	SI	El control esta implementado y se documentan en los formatos de TI desarrollo y /o actualizacion de software.
	A.14.3.1	Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.

Relaciones con los proveedores	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	SI	El control esta implementado pero se debe reforzar, ya que en varias ocasiones se detecta que no se realiza seguimiento ni auditoria la prestación de los servicios por parte de los proveedores.
	A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
Gestión de incidentes de seguridad de la información	A.16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.

Aspectos de seguridad de la información de la gestión de continuidad de negocio	A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
Cumplimiento	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.	SI	El control esta implementa y se encuentra dentro de la normatividad de la entidad.
	A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.18.1.3	Protección de registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	SI	El control esta implementado y se puede encontrar a través del manual de politica de seguridad para el manejo de la información
	A.18.1.4	Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.18.1.5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	NO	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.
	A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	SI	El control esta implementado, el área de control interno realiza auditorias sobre los diferentes procesos del área de TI.
	A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	SI	El control esta implementado pero falta más evidencia.
	A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI	El control no esta implementado, no se encuentra documentación o procedimientos establecidos donde se aplique este control.

Fuente: El autor

Fase 3 – Definición de estrategias para prevención de ciberataques en el ICPJ: En esta fase una vez conocido el estado de los controles para la seguridad de la información en el ICPJ y cuáles son los activos de información en la entidad que tienen un riesgo de valoración alta o superior, se procede a definir una serie de recomendaciones y acciones que permitan mitigar los riesgos identificados con el fin de proteger la información crítica de la entidad:

Tabla 25. Definición de estrategias y/o recomendaciones para mitigar los riesgos con valoración alta o superior

Activo	Amenaza	Riesgo	Recomendaciones para el manejo del riesgo	Acciones a realizar
Sistema de información misional	Errores de configuración	Perdida de disponibilidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 -A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Revisar y actualizar la política de seguridad de la información, guardar un log de eventos con las acciones realizadas en el sistema de información, documentar cualquier cambio de configuración que se realice en el sistema, contar con un ambiente de pruebas para ejecutar cualquier acción que requiera permisos de administrador antes de replicar las acciones en el sistema principal.
	Equivocaciones por parte del administrador del sistema	Perdida de confidencialidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 - A.9.2.3- A.9.2.4 - A.9.2.5 - A.9.3.1 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.11.2.4 - A.12.1.1 - A.12.4.3	Implementar y realizar un seguimiento de eventos de toda actividad que el administrador ejecute en el sistema. Definir responsabilidades y controles de accesos para el administrador.
	Intrusión de código malicioso	Perdida de disponibilidad e integridad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.6.2.1 - A.6.2.2 - A.8.1.3 - A.8.2.3 - A.8.3.1 - A.8.3.2 - A.8.3.3 - A.9.1.1 - A.9.1.2 - A.9.2.1 - A.9.2.2 - A.9.2.3 -A.9.2.4 - A.9.2.5 - A.9.2.6 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.1 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.2.1 - A.13.1.1 - A.13.1.2 - A.13.1.3 A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Actualizar el sistema operativo sobre el cual opera el sistema de información misional, actualizar la versión de Java que hace uso el sistema, restringir su uso para que solo se pueda acceder dentro de la red de la entidad, cambiar el protocolo http a https, renovar la contraseña de todos los usuarios cada 30 días, la contraseña debe contener como mínimo 15 caracteres se debe contener letras mayúsculas, minúsculas, números y caracteres especiales, mantener el software antivirus actualizado y con protección contra manipulaciones.

Software base datos	Intrusión de código malicioso	Perdida de disponibilidad e integridad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.6.2.1 - A.6.2.2 - A.8.1.3 - A.8.2.3 - A.8.3.1 - A.8.3.2 - A.8.3.3 - A.9.1.1 - A.9.1.2 - A.9.2.1 - A.9.2.2 - A.9.2.3 -A.9.2.4 - A.9.2.5 - A.9.2.6 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.1 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.2.1 - A.13.1.1 - A.13.1.2 - A.13.1.3 A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Actualizar la versión de software de base de datos Oracle pues es muy antiguo, modificar la contraseña de administrador cada 30 días, la contraseña debe contener como mínimo 15 caracteres se debe contener letras mayúsculas, minúsculas, números y caracteres especiales. mantener el sistema operativo sobre el cual opera la base de datos actualizado, mantener el software antivirus actualizado y con protección contra manipulaciones.
Software de gestión documental ORFEO	Errores de configuración	Perdida de disponibilidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 -A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Revisar y actualizar la política de seguridad de la información, guardar un log de eventos con las acciones realizadas en el sistema de información, documentar cualquier cambio de configuración que se realice en el sistema, contar con un ambiente de pruebas para ejecutar cualquier acción que requiera permisos de administrador antes de replicar las acciones en el sistema principal.
	Errores de mantenimiento	Perdida de disponibilidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 -A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Revisar y actualizar la política de seguridad de la información, guardar un log de eventos con las acciones realizadas en el sistema de información, documentar cualquier cambio de configuración que se realice en el sistema, contar con un ambiente de pruebas para ejecutar cualquier acción que requiera permisos de administrador.
	Equivocaciones por parte del administrador del sistema	Perdida de confidencialidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 - A.9.2.3- A.9.2.4 - A.9.2.5 - A.9.3.1 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.11.2.4 - A.12.1.1 - A.12.4.3	Implementar y realizar un seguimiento de eventos de toda actividad que el administrador ejecute en el sistema. Definir responsabilidades y controles de accesos para el administrador.

Software de sistemas operativos	Intrusión de código malicioso	Perdida de disponibilidad e integridad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.6.2.1 - A.6.2.2 - A.8.1.3 - A.8.2.3 - A.8.3.1 - A.8.3.2 - A.8.3.3 - A.9.1.1 - A.9.1.2 - A.9.2.1 - A.9.2.2 - A.9.2.3 -A.9.2.4 - A.9.2.5 - A.9.2.6 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.1 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.2.1 - A.12.5.1- A.12.6.1 - A.12.6.2 - A.13.1.1 - A.13.1.2 - A.13.1.3 A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Mantener los sistemas operativos actualizados con todos los parches suministrador por Microsoft, instalar un servidor WSUS para replicar de manera eficaz y eficiente las actualizaciones en los sistemas operativos, mantener el software antivirus actualizado y con protección contra manipulaciones, para los sistemas operativos obsoletos teniendo en cuenta el presupuesto de la entidad se debe actualizar a un sistema operativo GNU/Linux.
Software de virtualización	Intrusión de código malicioso	Perdida de disponibilidad e integridad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.6.2.1 - A.6.2.2 - A.8.1.3 - A.8.2.3 - A.8.3.1 - A.8.3.2 - A.8.3.3 - A.9.1.1 - A.9.1.2 - A.9.2.1 - A.9.2.2 - A.9.2.3 -A.9.2.4 - A.9.2.5 - A.9.2.6 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.1 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.2.1 - A.13.1.1 - A.13.1.2 - A.13.1.3 A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Actualizar la versión del software de virtualización pues es muy antiguo, mantener el software antivirus actualizado y con protección contra manipulaciones y el sistema operativo donde funciona dicho software de virtualización con todos los parches actuales.
Software para copias de respaldo Veeam Backup	Intrusión de código malicioso	Perdida de disponibilidad e integridad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.6.2.1 - A.6.2.2 - A.8.1.3 - A.8.2.3 - A.8.3.1 - A.8.3.2 - A.8.3.3 - A.9.1.1 - A.9.1.2 - A.9.2.1 - A.9.2.2 - A.9.2.3 -A.9.2.4 - A.9.2.5 - A.9.2.6 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.1 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.2.1 - A.13.1.1 - A.13.1.2 - A.13.1.3 A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Actualizar la versión del software de virtualización pues es muy antiguo, mantener el software antivirus actualizado y con protección contra manipulaciones y el sistema operativo donde funciona dicho software de virtualización con todos los parches actuales.

Software para el control de inventarios	Errores de configuración	Perdida de disponibilidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 -A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Revisar y actualizar la política de seguridad de la información, guardar un log de eventos con las acciones realizadas en el sistema de información, documentar cualquier cambio de configuración que se realice en el sistema, contar con un ambiente de pruebas para ejecutar cualquier acción que requiera permisos de administrador antes de replicar las acciones en el sistema principal.
	Equivocaciones por parte del administrador del sistema	Perdida de confidencialidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 - A.9.2.3- A.9.2.4 - A.9.2.5 - A.9.3.1 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.11.2.4 - A.12.1.1 - A.12.4.3	Implementar y realizar un seguimiento de eventos de toda actividad que el administrador ejecute en el sistema. Definir responsabilidades y controles de accesos para el administrador.
	Intrusión de código malicioso	Perdida de disponibilidad e integridad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.6.2.1 - A.6.2.2 - A.8.1.3 - A.8.2.3 - A.8.3.1 - A.8.3.2 - A.8.3.3 - A.9.1.1 - A.9.1.2 - A.9.2.1 - A.9.2.2 - A.9.2.3 -A.9.2.4 - A.9.2.5 - A.9.2.6 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.1 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.2.1 - A.13.1.1 - A.13.1.2 - A.13.1.3 A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Actualizar la versión del software de virtualización pues es muy antiguo, mantener el software antivirus actualizado y con protección contra manipulaciones y el sistema operativo donde funciona dicho software de virtualización con todos los parches actuales.
Controlador de dominio	Equivocaciones por parte del administrador del sistema	Perdida de confidencialidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 - A.9.2.3- A.9.2.4 - A.9.2.5 - A.9.3.1 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.11.2.4 - A.12.1.1 - A.12.4.3	Implementar y realizar un seguimiento de eventos de toda actividad que el administrador ejecute en el sistema. Definir responsabilidades y controles de accesos para el administrador.
Controlador de dominio alterno	Equivocaciones por parte del administrador del sistema	Perdida de confidencialidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 - A.9.2.3- A.9.2.4 - A.9.2.5 - A.9.3.1 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.11.2.4 - A.12.1.1 - A.12.4.3	Implementar y realizar un seguimiento de eventos de toda actividad que el administrador ejecute en el sistema. Definir responsabilidades y controles de accesos para el administrador.

Portal Institucional	Abuso de privilegios de acceso	Perdida de confidencialidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 - A.9.2.3- A.9.2.4 - A.9.2.5 - A.9.3.1 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.11.2.4 - A.12.1.1 - A.12.4.3	Revisar y actualizar la política de seguridad de la información, definir y documentar las responsabilidades que tienen los usuarios frente a cualquier abuso de privilegios en el sistema.
	Acceso no autorizado	Perdida de confidencialidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 - A.9.2.3- A.9.2.4 - A.9.2.5 - A.9.3.1 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.11.2.4 - A.12.1.1 - A.12.4.3	Implementar y realizar un seguimiento de eventos de toda actividad que el administrador ejecute en el sistema. Definir responsabilidades y controles de accesos para el administrador.
	Errores de configuración	Perdida de disponibilidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 -A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Revisar y actualizar la política de seguridad de la información, guardar un log de eventos con las acciones realizadas en el sistema de información, documentar cualquier cambio de configuración que se realice en el sistema, contar con un ambiente de pruebas para ejecutar cualquier acción que requiera permisos de administrador antes de replicar las acciones en el sistema principal.
	Errores de mantenimiento	Perdida de disponibilidad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.8.1.3 - A.8.2.3 -A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	Revisar y actualizar la política de seguridad de la información, guardar un log de eventos con las acciones realizadas en el sistema de información, documentar cualquier cambio de configuración que se realice en el sistema, contar con un ambiente de pruebas para ejecutar cualquier acción que requiera permisos de administrador.
	Vulnerabilidades de página web	Perdida de disponibilidad e integridad	A través de los controles relacionados a continuación se realiza la mitigación del riesgo: A.5.1.1- A.5.1.2 - A.6.1.1- A.6.1.2 - A.6.1.3 - A.6.1.4 - A.6.1.5 - A.6.2.1 - A.6.2.2 - A.8.1.3 - A.8.2.3 - A.8.3.1 - A.8.3.2 - A.8.3.3 - A.9.1.1 - A.9.1.2 - A.9.2.1 - A.9.2.2 - A.9.2.3 -A.9.2.4 - A.9.2.5 - A.9.2.6 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.9.4.4 - A.9.4.5 - A.10.1.1 - A.10.1.2 - A.12.1.1 - A.12.1.2 - A.12.1.3 - A.12.1.4 - A.12.2.1 - A.13.1.1 - A.13.1.2 - A.13.1.3	Actualizar el sistema operativo sobre el cual opera la página web, cambiar el protocolo http por https, actualizar la tecnología que usa la página web pues es antigua, mantener el software antivirus actualizado y con protección contra manipulaciones.

			A.12.6.1 - A.12.7 - A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7 - A.17.1.2	

Fuente: El autor

8. NUEVAS ÁREAS DE ESTUDIO

Trabajo De Grado

Desarrollado por estudiantes de postgrado como requisito para obtener el título de especialista en seguridad de la información. Es un estudio limitado y sistemático acerca de un área de acuerdo con un manejo eficaz de la bibliografía que este contiene y que se enfoca en particular en un modelo conceptual y practico utilizando una metodología especifica con la cual se detalle un nivel apropiado para el objeto de estudio de la seguridad de la información en la empresa ICPJ, de acuerdo a que los resultados obtenidos por la implementación de la evaluación de riesgos realizada en el ICPJ permitió conocer muchas falencias y como poder mitigarlas, se puede continuar con el desarrollo del presente trabajo de grado en pro de mejorar la seguridad de los demás activos de información de la entidad a través de una evaluación de riesgos más profunda.

Publicación Repositorio Universidad

Se realizará la publicación del trabajo de grado en el repositorio de la Universidad Católica de Colombia como medio de comunicación en la internet.

Presentación Jurados

Se realizará un trabajo de grado que se presentará ante el comité académico que está compuesto por un grupo de profesores de la Universidad Católica de Colombia como medio de evaluación y divulgación de la propuesta para la mejora de la seguridad de la información en la empresa ICPJ.

Reuniones Virtuales

Se utilizarán medios electrónicos para socializar el avance del proyecto mediante reuniones virtuales con el ICPJ, con el fin de proteger de la mejor manera su información critica la entidad podrá continuar desarrollando el presente proyecto tomando como área de estudio la evaluación de riesgos y la ciberseguridad.

9. CONCLUSIONES

En el desarrollo del presente proyecto se llevaron acciones en conjunto con el área de tecnología del ICPJ para proteger la información crítica de la entidad, acciones como: la actualización de los sistemas operativos donde estaba funcionando el sistema de información misional SIM y la página web de la entidad, de Windows Server 2003 sistema operativo obsoleto desde el año 2015, se realizó la actualización por Windows Server 2016, también se reemplazó el sistema operativo en 400 computadores, de Windows XP un sistema operativo obsoleto desde el año 2014 por Debian 10 Buster, esto permitió que muchas amenazas informáticas no tuvieran ningún efecto en estos equipos de cómputo ni en la red de la entidad pues dichas amenazas fueron especialmente diseñadas y creadas para atacar a los sistemas Windows, también se implementó un servidor WSUS con el fin de tener actualizados todos los sistemas operativos Windows 7, 8 y 10 con los cuales cuenta la entidad.

Se inhabilitaron los usuarios administradores locales de los computadores, el tiempo para cambiar la contraseña de todos los usuarios del dominio se modificó de 60 días a 30, de igual manera la longitud de la contraseña también se cambió quedando como requisito tener un mínimo de 12 caracteres entre mayúsculas, minúsculas, números y signos, se habilito el bloqueo de sesión automático por inactividad y por números de intentos errados, planes de concientización constante a los usuarios de la entidad sobre la seguridad de la información, también se implementó el factor de doble autenticación en activos como el SIM, correo electrónico y Orfeo. Todas estas acciones permitieron reducir considerablemente el número de amenazas las cuales iban rápidamente en aumento en los últimos 4 años, en el año 2019 fueron detectadas 27699 amenazas como ransomware, troyanos, phishing, spyware, entre otras y a la fecha 10 de noviembre de 2020 fueron detectadas 13888, es importante recalcar que en los últimos 4 años el ICPJ entre las 2 últimas semanas del mes de octubre y la 1 semana de noviembre era una víctima recurrente por parte de ciberataques inhabilitando muchos servicios primordiales de la entidad como el sistema SIM, pero debido a la implementación de todas las acciones que se ejecutaron en conjunto con el área de TI en este año, ningún activo de información crítico del ICPJ fue víctima de estos ataques.

10. BIBLIOGRAFÍA

[1] KASPERSKI, Yevgueni, **"**¿Qué es la ciberseguridad?". Consultado 01 marzo de 2020, disponible desde Internet en:
https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[2] HIGHAM, Greg, "Todo acerca del malware", Consultado 01 marzo de 2020 disponible desde Internet en:
https://es.malwarebytes.com/malware/

[3] SNOW, John. 07 de noviembre de 2018. "Top 5 de los ciberataques más memorables". Consultado 12 marzo de 2020, disponible desde Internet en:
https://www.kaspersky.es/blog/five-most-notorious-cyberattacks/17277/

[4] LIPOVSKY, Robert, 20 de junio de 2017. "A siete años de Stuxnet, los sistemas industriales están nuevamente en la mira". Consultado 12 marzo de 2020, disponible desde Internet en:
https://www.welivesecurity.com/la-es/2017/06/20/sistemas-industriales-en-la-mira/

[5] DROZHZHIN, Alex, 10 de noviembre de 2014. "DarkHotel: una campaña de espionaje en hoteles de lujo asiáticos". Consultado 12 marzo de 2020, disponible desde internet en:
https://www.kaspersky.es/blog/darkhotel-espionaje-en-hoteles-de-lujo-asiaticos/4809/

[6] KHALIMONENKO, Alexander, Strohschneider, Jens, Kupreev, Oleg, 02 de febrero de 2017, "DDoS attacks in Q4 2016". Consultado 12 marzo de 2020 disponible desde Internet en:
https://securelist.com/ddos-attacks-in-q4-2016/77412/

[7] AVAST, "WannaCry". Consultado 12 marzo de 2020 disponible desde Internet en: https://www.avast.com/es-es/c-wannacry

[8] BELCIC, Ivan, 28 de noviembre de 2019. "¿What is Petya Ransomware, and Why is it so Dangerous?". Consultado 12 marzo de 2020 disponible desde Internet en: https://www.avast.com/c-petya

[9] AVAST, "Phishing". Consultado 12 marzo de 2020 disponible desde Internet en: https://www.avast.com/es-es/c-phishing

[10] SONICWALL, 28 de mayo de 2019. "Dentro de las campañas de phishing modernas de 2019". Consultado 12 marzo de 2020, disponible desde internet en:
https://blog.sonicwall.com/es-mx/2019/05/inside-the-modern-phishing-campaigns-of-2019/

[11] EUROPAPRESS, 07 agosto 2019. “El ataque DDoS más largo de la historia ha sido en 2019 y duró 509 horas”. Consultado 12 marzo de 2020, disponible desde Internet en:
https://www.europapress.es/portaltic/ciberseguridad/noticia-ataque-ddos-mas-largo-historia-sido-2019-duro-509-horas-20190807160911.html

[12] IBRAGIMOV, Timur, KUPREEV, Oleg, EKATERINA, Badovskaya, GUTNIKOV, Alexander, 11 de noviembre de 2019. “Los ataques DDoS en el tercer trimestre de 2019”. Consultado 12 marzo de 2020 disponible desde Internet en:
https://securelist.lat/ddos-report-q3-2019/89671/

[13] IONOS, 19 de marzo de 2019, Consultado 12 marzo de 2020, disponible desde Internet en:
https://www.ionos.es/digitalguide/servidores/seguridad/ataques-man-in-the-middle-un-vistazo-general/

[14] BARRIOS,Joel, 06 diciembre 2019. “MITM Ataque Man In The Middle”, Consultado 12 marzo de 2020 disponible desde Internet en:
https://www.unfantasmaenelsistema.com/2019/12/mitm-ataque-man-in-the-middle/

[15] Policía Nacional de Colombia, Tendencias cibercrimen 2019 - 2020, En línea, Consultado 12 marzo de 2020 disponible en:
https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

[16] Microsoft, “Finalizó el soporte técnico para Windows XP”. Consultado 12 marzo de 2020 disponible desde Internet en:
https://www.microsoft.com/es-co/microsoft-365/windows/end-of-windows-xp-support

[17] KARLSSON LLORENS, Cecilia, 14 de mayo de 2019. “Fin del soporte a Windows Server 2003”. Consultado 12 marzo de 2020 disponible desde Internet en:
https://www.ciset.es/publicaciones/blog/311-fin-del-soporte-a-windows-server-2003

[18] Microsoft, “El soporte para Windows Server 2008 ha finalizado”. Consultado 12 marzo de 2020 disponible en:
https://www.microsoft.com/es-es/cloud-platform/windows-server-2008

[19] Microsoft, 15 de enero de 2020. “El soporte de Windows 7 finalizó el 14 de enero de 2020”. Consultado 12 marzo de 2020 disponible en:
https://support.microsoft.com/es-co/help/4057281/windows-7-support-ended-on-january-14-2020

[20] GONZALEZ, Eduardo. que-es-un-ciberataque-y-tipos, página web, Consultado 12 marzo de 2020 disponible en: https://www.caser.es/seguros-empresas/articulos/que-es-un-ciberataque-y-tipos

[21] CEBALLOS, Adriana. Tendencias cibercrimen en Colombia. En línea. 29 octubre de 2019. 23 abril 2020. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[22] GEMA, Gasco. Seguridad informática: Software malicioso. Segunda edición. Madrid: MACMILLAN, 2013. 113p.

[23] Jaén, Universidad. Guías de seguridad UJA. En línea. 2 febrero 2018. 25 abril de 2020. Disponible en: https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%206.%20Ransomware.pdf

[24] GEMA, Gasco. Seguridad informática: Software malicioso. Segunda edición. Madrid: MACMILLAN, 2013. 12p.

[25] WALTER, Velasco. Políticas y seguridad de información. En línea. 2 septiembre de 2008. 26 abril de 2020. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

[26] AUCHARD, Eric. Descubren vulnerabilidad de routers cisco ante ataques informáticos. En línea. 15 septiembre de 2015. 27 de abril de 2020. Disponible en: https://lta.reuters.com/articulo/internet-tecnologia-cisco idLTAKCN0RF19620150915

[27] MONSALVE, Julián. Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento, Boyacá. 2014. 72 páginas. Trabajo de grado. Universidad Santo Tomas. Tunja.

[28] MORA, David. Técnicas de ofensa y defensa a los fallos por corrupción de memoria. Medellín. Trabajo de grado. Universidad de Medellín.

[29] URBINA, Gabriel. Introducción a la Seguridad informática. Segunda edición: San Juan,2016. 160 p.

[30] HURTADO, Mario. Análisis de Certificados SSL/TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación. En línea. 10 de febrero de 2017. 8 abril de 2020. Disponible en:

http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-65422017000100273

[31] FABIAN, Buendía. Seguridad informática. Primera edición. Madrid: MCGRAW HILL, 2013. 212p.

[32] AMARO, José. Seguridad en internet. En línea. 2 febrero de 2017. 7 abril de 2020. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072017000100006

[33] HERRERA, John. Las vulnerabilidades de seguridad de DNS. En línea. 14 febrero de 2018. 5 abril de 2020. Disponible en: https://www.researchgate.net/publication/320985758_Las_vulnerabilidades_de_seguridad_de_DNS

[34] PUIG, Toni, Identificación de ataques y técnicas de intrusión. En línea. 27 enero de 2010. 4 de abril de 2020. Disponible en: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/203/A5.pdf?sequence=5

[35] INTECO, Análisis de tráfico con wireshark. En línea. 24 de marzo de 2010. 7 de abril de 2020. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

[36] VOUTSSAS, Juan. Preservación documental digital y seguridad informática. En línea. 6 de abril de 2010. 10 abril de 2020. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

[37] DIAZ, Jairo. Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. En línea. 01 de octubre de 2019. 4 abril de 2020. Disponible en: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872019000200006

[38] BETANCOURT, Carlos. Ciberseguridad en los sistemas de información de las universidades. 22 agosto 2017. Consultado 12 marzo de 2020. Disponible en: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

[39] CALVELLO, Mara. Tendencias de ciberseguridad para 2020. En línea. 17 de febrero 2020. 20 de marzo de 2020. Disponible en: https://jaxenter.com/cybersecurity-trends-2020-167575.html

[40] VERGELIS, Maria. Spam y phishing en el tercer trimestre de 2019. En línea. 26 noviembre de 2019. Consultado 20 marzo de 2020. Disponible en: https://securelist.lat/spam-report-q3-2019/89777/.

[41] SANTIAGO, Castro. En línea. La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones. 23 de abril de 2018. Consultado el 20 marzo 2020.Disponible en:
https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

[42] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, Ciberseguridad. En línea, 26 diciembre 2019. Consultado 12 marzo de 2020 disponible en:
https://www.mintic.gov.co/portal/inicio/Micrositios/I+D+I/Nodos/6120:Ciberseguridad

[43] Revista Dinero, Ciberseguridad, web,12 marzo de 2019. Consultado 14 marzo de 2020 disponible: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

[44] JOYANES, Luis. Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial. 4 edición. Madrid: Alfaomega, 2017, 32 p.

[45] Diario oficial, Ley 1273 de 2009. En línea. 5 enero de 2009. 17 marzo 2020. Disponible en:
https://www.armada.mil.co/sites/default/files/normograma_arc/telematica/Ley%201273%20de%202009%20Modifica%20CP%20para%20protecci%C3%B3n%20de%20datos%20e%20informaci%C3%B3n.pdf

[46] Congreso de Colombia, En línea. 5 enero de 2009. 18 marzo 2020. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

[47] MARÍA, Hoyos. Decreto 000103. En línea. enero 20 de 2015. Abril 25 de 2020. Disponible en:
www-leyex-info.ucatolica.basesdedatosezproxy.com/documents/leyes/Decreto103de2015.pdf

[48] MOLANO, Diego. Ley 1581 de 2012. En línea. 17 octubre de 2012. 25 abril de 2020. Disponible en: https://ucatolica-leyex-info.ucatolica.basesdedatosezproxy.com/normativa/detalle/ley-1581-de-2012-24760/pdf

[49] Cifuentes, Carlos. El debido proceso en la ley del habeas data. En línea. 21 abril de 2017. 25 abril de 2020. Disponible en:
http://www.scielo.org.co/pdf/cesd/v8n1/v8n1a11.pdf

[50] JOYANES, Luis. Introducción estado del arte de la ciberseguridad. En línea. 1 Julio de 2010. 18 marzo de 2020. Disponible en: https://dialnet.unirioja.es/descarga/articulo/3837217.pdf

[51] GEMA, Sánchez. Los estados y la ciberguerra. En línea. 23 octubre 2017. 20 de abril de 2020 Disponible en: https://es.scribd.com/document/362322056/Dialnet-LosEstadosYLaCiberguerra-3745519

[52] JOYANES, Luis. Estado del arte de la ciberseguridad. En línea. 1 julio de 2010. 19 de abril de 2020. Disponible en: Dialnet-IntroduccionEstadoDelArteDeLaCiberseguridad-3837217%20(3).pdf

[53] ALEJANDRO, Estrada Ciber amenazas 2013 y tendencias 2014. En línea. 20 de octubre de 2014. 4 abril de 2020. Disponible en: www.ccn-cert.cni.es/publico/dmpublidocuments/CCN-CERT_IA-03-14-Ciberamenazas_2013_Tendencias_2014-publico.pdf

[54] CNN, Yahoo sufre un ataque cibernético masivo que compromete cuentas de correo. En línea. 31 enero de 2014. 12 abril de 2020. Disponible en: https://cnnespanol.cnn.com/2014/01/31/yahoo-sufre-un-ataque-cibernetico-masivo-que-compromete-cuentas-de-correo/

[55] CLAVIJO, Felipe. Riesgo cibernético. En línea. 2 julio de 2017. 25 marzo de 2020. Disponible en: https://www.banrep.gov.co/sites/default/files/publicaciones/archivos/rref_recuadro_7_2017.pdf

[56] POLLARD, Jeff. Botnet Mirai. En línea. 24 octubre de 2016. 20 de abril de 2020. Disponible en: https://www.akamai.com/es/es/multimedia/documents/white-paper/akamai-mirai-botnet-and-attacks-against-dns-servers-white-paper.pdf

[57] Actualidad, Seis ataques cibernéticos que sacudieron al mundo. En linea.5 enero de 2019. Disponible en: https://www.dw.com/es/seis-ataques-cibern%C3%A9ticos-que-sacudieron-el-mundo/a-46967214

[58] MUÑOZ, Camilo. Análisis de metodologías de ethical hacking para la detección de vulnerabilidades en las pymes. En línea. 24 julio de 2019. 26 abril de 2020 de 2020. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/30302/ccpenagosm.pdf?sequence=1&isAllowed=y

[59] GONZÁLEZ, María. Protocolo de gestión de vulnerabilidades. En línea. 2 febrero de 2019. 27 abril de 2020. Disponible en: http://bibing.us.es/proyectos/abreproy/92187/fichero/TFG-2187-GONZALEZ.pdf

[60] GÓMEZ, Antonio. Herramientas básicas del hacker. En línea. 2 marzo 2015. 10 abril de 2020. Disponible en: https://ucys.ugr.es/download/taller3/Taller3_Metasploit_Part1.pdf

[61] EVAN, Dunbar. what-is-kali-linux. En línea, Consultado 15 marzo de 2020 disponible en: https://www.educative.io/edpresso/what-is-kali-linux